WARWICK
THE UNIVERSITY OF WARWICK

A Thesis Submitted for the Degree of PhD at the University of Warwick

Permanent WRAP URL:
http://wrap.warwick.ac.uk/107557

Copyright and reuse:
This thesis is made available online and is protected by original copyright.
Please scroll down to view the document itself.
Please refer to the repository record for this item for information to help you to cite it.
Our policy information is available from the repository home page.

For more information, please contact the WRAP Team at: wrap@warwick.ac.uk

warwick.ac.uk/lib-publications

THE BRITISH LIBRARY
BRITISH THESIS SERVICE

TITLE PRIME-POWER LIE ALGEBRAS AND FINITE P-GROUPS.

AUTHOR Paul Jonathon SANDERS

DEGREE Ph.D

AWARDING BODY Warwick University

DATE 1994

THESIS NUMBER DX187307

THIS THESIS HAS BEEN MICROFILMED EXACTLY AS RECEIVED

The quality of this reproduction is dependent upon the quality of the original thesis submitted for microfilming. Every effort has been made to ensure the highest quality of reproduction. Some pages may have indistinct print, especially if the original papers were poorly produced or if awarding body sent an inferior copy. If pages are missing, please contact the awarding body which granted the degree.

Previously copyrighted materials (journals articles, published texts etc.) are not filmed.

This copy of the thesis has been supplied on condition that anyone who consults it is understood to recognise that it's copyright rests with its author and that no information derived from it may be published without the author's prior written consent.

Reproduction of this thesis, other than as permitted under the United Kingdom Copyright Designs and Patents Act 1988, or under specific agreement with the copyright holder, is prohibited.

Prime-Power Lie Algebras and Finite p-groups

by

Paul Jonathon Sanders

A thesis submitted to the University of Warwick
for the degree of Doctor of Philosophy

Mathematics Institute, University of Warwick

September 1994

Table of Contents.

Acknowledgements.

Firstly, I would like to thank my Ph.D. supervisor Dr. John Moody for introducing me to the topic of finite p-groups, for suggesting interesting and stimulating problems, and for mathematical advice and discussions during the research and writing periods associated with this thesis.

The initial two years of research for this thesis was funded mostly by a grant from the Science and Engineering Research Council supplemented by income from the supervision system at Warwick. For the third year, I would like to thank my parents for their generosity, and to the Mathematics Department of the University of Warwick for the award of a small assistance grant.

I would also like to thank my undergraduate personal tutor Dr. Geoff Smith of the University of Bath for inspiring me to pursue a research degree. Finally, I would like to thank the people I have become good friends with while at Warwick for their support (and in certain cases, for the use of some of their TEX macros).

Declaration.

The material in this thesis is, to the best of my knowledge, original except where otherwise stated. Particular attention should be drawn to sections 1·1 (and its subsections), and 1·2 which consist of entirely expositiory material. The research for chapter 2 was a joint collaboration between myself and Dr. Tom Wilde, and both parties contributed to this research in equal proportions.

Summary.

In this thesis we use the Lie ring functors of Magnus and Lazard to investigate finite p-groups which possess either a cyclic subgroup of small index, or whose derived subgroup has exponent dividing p. The class of groups we consider is sufficiently large to include completely 11 of the 15 families of groups of order p^7 ($p \geq 7$), partitioned by Hall's type invariants. Some information on the other 4 families is also derived.

Motivated by the work of Burnside [3] and Miller [21] concerning the stable behaviour of groups of order p^n and exponent p^{n-2} for p and n sufficiently large, we investigate the existence of stability for the number of isomorphism classes of groups of order p^n and exponent p^{n-f} as p and n vary, with f an arbitrary fixed integer greater than 2. To facilitate this, we allow finitely many specified primes to be excluded for each f at the outset. The approach is to then consider the corresponding problem for p^n-element nilpotent Lie rings and use the Lie ring functors to recover a solution for the groups. A non–trivial step immediately arises in showing the existence of an initial set of excluded primes which are sufficient to enable the Lie ring functors to be invoked since they only apply when the prime is greater than the nilpotency class (of both the groups and Lie rings). This step is dealt with and explored in chapters 2 and 3.

In the main theorem of chapter 4 we show that for $f \geq 3$ the number of isomorphism classes of groups of order p^n and exponent p^{n-f} is independent of n for n sufficiently large and p not one of the excluded primes (which depend only on f). The excluded primes ensure regularity holds for such groups and the proof of this theorem yields precise stability results in terms of the corresponding type invariants. The method of proof shows explicitly how to construct the corresponding Lie rings, and in chapter 5 we utilise this procedure to produce a formula for the number of groups of order p^n and exponent p^{n-3} where $p \geq 5$ and $n \geq 7$. The precise stability results of chapter 4 enable us to reduce some of the calculations to the known classification of groups of order p^5 ($p \geq 5$).

On the other hand, in chapter 6 we use the Lie ring functors to solve a restricted form of a conjecture of J. Moody [22] by exhibiting, for a prime p greater than or equal to the positive integer n, a natural, but not functorial, one-to-one correspondence between isomorphism classes of finite groups of order p^n whose derived subgroup has exponent dividing p, and isomorphism classes of nilpotent $\mathsf{F}_p[T]/(T^n)-$Lie algebras L of F_p-dimension n in which $T[L,L] = 0$. By viewing such an algebra as a nilpotent F_p-Lie algebra equipped with a nilpotent element of its centroid one obtains a "formula" for the number of such groups. This applies, in particular, to the groups of order p^7 since the 7-dimensional nilpotent F_p-Lie algebras are known from [30] (and the Magnus–Lazard functors) for $p \geq 7$. In view of current interest in these groups, we conclude with a summary of the information contained in this thesis on groups of order p^7.

Chapter 1. Lie Rings and Regular p-Groups

Throughout this thesis we will be repeatedly using a functorial correspondence between certain families of Lie rings and p-groups. In order to make this thesis reasonably self-contained we include an exposition in section 1·1 of this correspondence with particular emphasis on the the situation we are interested in (namely finite p-groups). This section also contains the relevant definitions and notation which we will be using concerning Lie rings and algebras. The exposition we give is a condensed form of the paper [15] and should be consulted for any additional information.

Since we will be dealing substantially with regular p-groups, section 1·2 is devoted to collating the relevant definitions, notation and classical theorems for this family of p-groups taken from the paper [7] of P. Hall.

We conclude this chapter with an immediate application of the Lie ring correspondence to answer a question posed in [7] concerning bases of regular p-groups.

Section 1·1. Lie Rings.

Section 1·1·1. Definitions and Introduction.

Let C be a commutative ring with 1 and suppose that A is a (unital) C-module. A is called a **C-algebra** if there exists a multiplication $[.,.] : A \times A \to A$ such that for any elements x, y, z of A and λ, μ of C we have

i) $[\lambda x + \mu y, z] = \lambda[x, z] + \mu[y, z]$

ii) $[x, \lambda y + \mu z] = \lambda[x, z] + \mu[y, z]$

In other words, the multiplication is given by an element of $\mathrm{Hom}_C(A \otimes_C A, A)$. If, in addition, $[[x, y], z]] = [x, [y, z]]$ for any $x, y, z \in A$ then A is called *associative*. A **C-Lie algebra** is defined to be a C-algebra A in which for any elements x, y, z of A we have

iii) $[x, x] = 0$

iv) $[[x, y], z] + [[y, z], x] + [[z, x], y] = 0$ (the *Jacobi identity*)

Such a multiplication is then called a Lie bracket on A (observe that the above conditions imply that $[x,y] = -[y,x]$ for any $x,y \in A$ so that a Lie bracket is skew-symmetric). If C is the ring of integers $\mathbb{Z}$ then a C-Lie algebra A is called a **Lie ring**, and in this case if there exists a prime p such that every element of A has additive order a power of p then we will call A a **p-Lie ring**.

Given two C-submodules U and V of a $C-$algebra A, we define $[U,V]$ to be the C-submodule of A spanned by the set $\{[u,v] : u \in U \text{ and } v \in V\}$, and a **$C-$subalgebra** of A is then defined to be a C-submodule U of A such that $[U,U] \subseteq U$. If U satisfies $[U,A] \subseteq U$ (resp. $[A,U] \subseteq U$) then we call U a **right (resp. left) ideal** of A, and if U is both a left and a right ideal then we call it an **ideal**. Observe that if the product in A is skew-symmetric then one-sided ideals are automatically two-sided ideals. If U is an ideal of A then the induced multiplication on the quotient C-module A/U is well-defined and yields a C-algebra structure which is associative (resp. Lie) if A is associative (resp. Lie). Given a subset X of A, the subalgebra generated by X is defined to be the intersection of all subalgebras of A which contain X and is denoted by $\langle X \rangle$. Similarly, the ideal generated by X is defined to be the intersection of all the ideals of A which contain X. A morphism between two C-algebras A and B is a C-homomorphism $\theta : A \to B$ such that for each $x,y \in A$ we have $\theta[x,y] = [\theta x, \theta y]$. The kernel K of such a map is easily seen to be an ideal of A and the quotient algebra A/K is isomorphic to the subalgebra θA of B.

Given an associative C-algebra A, a subset X of A is said to be an **associative basis** of A if $\langle X \rangle = A$ and any mapping of X into an arbitrary associative C-algebra B is the restriction of a C-algebra homomorphism from A into B. A is then said to be a free associative algebra. Similarly, if L is a C-Lie algebra then a subset X of L is said to be a **Lie basis** of L if $\langle X \rangle = L$ and any mapping of X into an arbitrary C-Lie algebra M is the restriction of a C-algebra homomorphism from L into M. L is then said to be a free Lie algebra.

If X is any set of symbols then it is straightforward to construct an associative C-algebra which contains X as an associative basis; take the free C-module on the set of finite strings over X (i.e. the set $X^* = \{x_1 \dots x_n : n \geq 0, x_i \in X\}$) and define the multiplication between basis elements by juxtaposition (X^* becomes the free associative monoid with this

multiplication). This extends to give an associative C-algebra with X as an associative basis and is denoted by $C\langle X\rangle$. It is also possible to give a direct construction of a C-Lie algebra which contains X as a Lie basis (see [10]) although we can also obtain a free C-Lie algebra from the free associative C-algebra $C\langle X\rangle$ in the following manner. If A is an associative C-algebra (where we denote the multiplication by juxtaposition) then we can define a C-Lie algebra structure on A by defining the bracket of two elements x, y of A to be $xy - yx$. It is not difficult to verify that this defines a Lie bracket and the resulting Lie algebra will be denoted by A_L. In the case when A is $C\langle X\rangle$ then the Lie subalgebra of A_L generated by X has X as a Lie basis. A proof of this fact in the case that C is a field or the ring of integers $\mathbb{Z}$ can be found in [10]. An element a of $C\langle X\rangle$ is then called a ***Lie element*** if a belongs to the Lie subalgebra generated by X.

Now let L be a C-Lie algebra. If $x_1, \ldots, x_n$ are elements of L with $n \geq 3$ then we define the symbol $[x_1, \ldots, x_n]$ inductively to mean the element $[[x_1, \ldots, x_{n-1}], x_n]$; this is the left-normed notation for Lie brackets. The centre of L is defined to be the ideal $Z(L) = \{z \in L : [x, z] = 0 \ \forall x \in L\}$, and then a chain $L = K_1 \geq K_2 \geq K_3 \cdots$ of ideals of L is called a descending central series of L if for each $i \geq 1$ we have $K_i/K_{i+1} \leq Z(L/K_{i+1})$, i.e. $[K_i, L] \leq K_{i+1}$. As with groups, we define the lower central series $\{\gamma_i(L)\}_{i\in\mathbb{N}}$ of L inductively by setting $\gamma_1(L) = L$ and $\gamma_{i+1}(L) = [\gamma_i(L), L]$ for $i \geq 1$. Since L is an ideal of L it follows from the Lie bracket axioms that this does indeed define a descending central series of L and moreover, if $\{K_i\}_{i\in\mathbb{N}}$ is any other descending central series of L we have $\gamma_i(L) \leq K_i$ for each i. If there exists some $c \geq 1$ such that $\gamma_{c+1}(L) = 0$ then L is called **nilpotent** and the minimum such c is called the nilpotency class $cl(L)$ of L. We call a C-Lie algebra L **Abelian** if $\gamma_2(L) = 0$ (which is equivalent to saying that L is nilpotent of class 1).

In the 1930's, W. Magnus and E. Witt were interested in studying the lower central series of free groups and, in order to simplify commutator calculations, introduced a technique of associating a Lie ring to a group. Their technique, now known as the Lie ring method, uses the fact that if a group G is given together with a **strongly** central series $G = G_1 \geq G_2 \geq G_3 \geq \cdots$ (i.e. for each $i, j \geq 1$, $[G_i, G_j] \leq G_{i+j}$), then for any $i, j \geq 1$

there exists a well-defined $\mathbf{Z}-$bilinear map

$$\sigma_{i,j} : {}^{G_i}/_{G_{i+1}} \times {}^{G_j}/_{G_{j+1}} \longrightarrow {}^{G_{i+j}}/_{G_{i+j+1}}$$

where $\sigma_{i,j}(xG_{i+1}, yG_{j+1}) = [x,y]G_{i+j+1}$ for any $x \in G_i$ and $y \in G_j$. The Lie ring is then constructed by using these bilinear maps to define the multiplication between homogeneous components of the graded $\mathbf{Z}-$module

$$L = \bigoplus_{i=1}^{\infty} {}^{G_i}/_{G_{i+1}}$$

which can then be extended in a unique way to a $\mathbf{Z}-$bilinear map $L \times L \to L$. The fact that L equipped with this multiplication satisfies the Jacobi identity follows from the ***Witt identity*** which states that in an arbitrary group any three elements x, y, z satisfy

$$[x, y^{-1}, z]^y [y, z^{-1}, x]^z [z, x^{-1}, y]^x = 1. \tag{1·1}$$

A full exposition of this method together with several applications can be found in [10] §VIII.

A disadvantage with this method is that by virtue of taking gradings, certain information about the group is lost. In particular, the correspondence is not one-to-one in the sense that non-isomorphic groups can give rise to isomorphic Lie rings. This is easily seen to be the case by considering the two non-Abelian groups of order p^3 and the Lie ring arising from the above construction.

The Lie ring correspondence that we will principally be using is again originally due to W. Magnus and seems to have first appeared in his paper [19] where the method is briefly described. Magnus's correspondence was also established independently by M. Lazard as a special case in his paper [15] although he acknowledges Magnus's earlier paper in a footnote ([15] p.180). Lazard's paper is very general and is concerned (in part) with investigating the circumstances under which a group structure can be defined on a rational Lie algebra by means of the Campbell–Hausdorff formula (see the next section). Moreover, he investigates the conditions under which this process can be inverted i.e. when can a Lie structure be defined on a group (by means of the group operation) in such a way that the

group structure is then recovered by using the Campbell–Hausdorff formula. As well as deducing the Magnus correspondence he also derives the Mal'cev correspondence between divisible torsion-free locally nilpotent groups and locally nilpotent rational Lie algebras as a special case (Mal'cev's original paper is [20]).

Magnus's paper [19] sketched how the Campbell–Hausdorff formula and its inversion process works in the context of finite nilpotent p-Lie rings and finite p-groups and it is this situation we are interested in. Given a finite nilpotent p-Lie ring U of nilpotency class less than p, the Campbell–Hausdorff formula can be used to define a group structure $\mathcal{G}_p(U)$ on U so that $\mathcal{G}_p(U)$ has nilpotency class less than p, and this procedure can be inverted in the sense that given a finite p-group P of nilpotency class less than p it is possible to define a Lie ring structure $\mathcal{L}_p(P)$ on P in such a way that $\mathcal{L}_p(P)$ is nilpotent of class less than p, with $\mathcal{G}_p(\mathcal{L}_p(P)) = P$ and $\mathcal{L}_p(\mathcal{G}_p(U)) = U$. If, for an arbitrary prime p, we denote by Λ_p the category of all finite nilpotent p-Lie rings which have nilpotency class less than p, and by Γ_p the category of all finite p-groups which have nilpotency class less than p), then $\mathcal{G}_p$ and $\mathcal{L}_p$ are mutually inverse covariant functors between Λ_p and Γ_p which preserve the underlying sets. As well as giving a strong functorial connection, $\mathcal{G}_p$ and $\mathcal{L}_p$ also preserve many structural properties. For instance, subgroups correspond to subrings, normal subgroups correspond to ideals and, in particular, any central series is preserved so that the nilpotency class of the group and its Lie ring coincides (and vice-versa).

Section 1·1·2 is a brief exposition of the part of Lazard's paper [15] which we are interested in and in section 1·1·3 we indicate how Lazard constructs the above functors. For full details, the paper [15] should be consulted.

Section 1·1·2. The Magnus Algebra and the Campbell–Hausdorff Formula.

In this section let X denote a finite set of symbols and $\mathbb{Q}$ the field of rational numbers. Following Cohn [4] we define a power series in X over $\mathbb{Q}$ to be a function $f : X^* \to \mathbb{Q}$ which will be denoted by the formal sum $\sum_{u \in X^*} f(u)u$; $f(u)$ is called the coefficient of u and $f(1)1$ is the constant term of f. The set of all such power series forms an associative $\mathbb{Q}$-algebra with 1 where addition and scalar multiplication are defined pointwise and multiplication of power series f, g is defined by

$$(fg)(u) = \sum_{v,w \in X^*} f(v)g(w), \text{ (a finite sum).}$$

This algebra is called the **Magnus algebra** (or the free algebra of formal power series in X over $\mathbb{Q}$) and is denoted by $\mathbb{Q}\langle\langle X \rangle\rangle$. It contains the free associative algebra $\mathbb{Q}\langle X \rangle$ as the subalgebra of elements with finite support (the support of an element f is defined to be the set $\text{supp}(f) = \{u \in X^* : f(u) \neq 0\}$), i.e. the polynomials in the non-commuting indeterminates X. $\mathbb{Q}\langle X \rangle$ can be regarded as a graded algebra where if $i \geq 0$ then we define the homogeneous elements of degree i to be the $\mathbb{Q}$-subspace H_i with basis $\{x_{j_1} \ldots x_{j_i} : x_{j_n} \in X \text{ for each } n\}$ (the associative monomials of degree i). Then, if $f \in \mathbb{Q}\langle\langle X \rangle\rangle$ and $i \geq 0$ we define its i^{th} homogeneous component to be $h_i(f) = \sum_{u \in H_i} f(u)u$ (an element of $\mathbb{Q}\langle X \rangle$), and if $f \neq 0$ we say that f has **order** $\omega(f)$ if $h_{\omega(f)}(f)$ is the first non-zero homogeneous component of f. We then denote by $I^{(i)}$ the collection of all elements f (together with 0) of $\mathbb{Q}\langle\langle X \rangle\rangle$ with $\omega(f) \geq i$ and this is seen to be an ideal of $\mathbb{Q}\langle\langle X \rangle\rangle$. This gives a descending chain of ideals of $\mathbb{Q}\langle\langle X \rangle\rangle$ with $\bigcap_{i \geq 0} I^{(i)} = \{0\}$. Using the order defined above we define a function

$$\begin{array}{rccl} |.| : & \mathbb{Q}\langle\langle X \rangle\rangle & \longrightarrow & \mathbb{R} \\ & f & \longmapsto & |f| = \begin{cases} 0, & \text{if } f = 0 \\ 2^{-\omega(f)}, & \text{if } f \neq 0 \end{cases} \end{array}$$

The following properties are then satisfied for any $f, g \in \mathbb{Q}\langle\langle X \rangle\rangle$

i) $|f| \geq 0$ with equality if and only if $f = 0$,

ii) $|f + g| \leq \max\{|f|, |g|\}$,

iii) $|fg| = |f| \cdot |g|$,

and so $|.|$ is a non-Archimedean absolute value on $\mathbb{Q}\langle\langle X\rangle\rangle$. From this valuation we obtain a metric which makes $\mathbb{Q}\langle\langle X\rangle\rangle$ into a complete topological algebra in which a series $\sum_{n=1}^{\infty} f_n$ of elements of $\mathbb{Q}\langle\langle X\rangle\rangle$ converges if and only if $f_n \to 0$. We can therefore regard a formal power series f as the limit of the series it defines and since the partial sums of such a series belong to $\mathbb{Q}\langle X\rangle$, we also see that $\mathbb{Q}\langle X\rangle$ is dense in $\mathbb{Q}\langle\langle X\rangle\rangle$.

Since $\mathbb{Q}\langle\langle X\rangle\rangle$ is associative it has an associated $\mathbb{Q}-$Lie algebra structure where if f and g are two elements then $[f,g] = fg - gf$. If L denotes the Lie subalgebra generated by X (so by the previous section this is free on X) then we denote the closure of L in $\mathbb{Q}\langle\langle X\rangle\rangle$ by $\overline{L}$. For $i \geq 1$, we define the non-associative words X_i in X of degree i inductively by setting $X_1 = X$ and for $i \geq 2$ we set

$$X_i = \bigcup_{j=1}^{i-1} X_j \times X_{i-j}$$

We then define a function $\pi : \cup_{i\geq 1} X_i \to L$ inductively by setting $\pi(x) = x$ for $x \in X_1$, and then if (u,v) is a word of degree $i > 1$ we set $\pi((u,v)) = [\pi(u), \pi(v)]$ ($\pi(u)$ and $\pi(v)$ having previously been defined). So π "evaluates" each non-associative word as a Lie element of $\mathbb{Q}\langle X\rangle$. A simple induction then shows that for any $i \geq 1$, $\pi(X_i) \subseteq H_i$, and are called the Lie monomials in X of degree i. For $i \geq 1$ we denote by K_i the $\mathbb{Q}$-subspace spanned by the Lie monomials of degree i and then we have $L = \bigoplus_{i\geq 1} K_i$ so that for each $i \geq 1$, $K_i = L \cap H_i$ (using the Jacobi identity it is possible to show that K_i is in fact spanned by the left-normed Lie monomials of degree i). It now follows that an element $f \in I^{(1)}(\mathbb{Q}\langle\langle X\rangle\rangle)$ lies in $\overline{L}$ if and only if $h_i(f) \in K_i$ for each $i \geq 1$.

Note. If we regard $\mathbb{Z}$ as a subring of $\mathbb{Q}$ then $\mathbb{Z}\langle X\rangle$ can be regarded as a subring of $\mathbb{Q}\langle X\rangle$ and the Lie subring E of $\mathbb{Z}\langle X\rangle$ generated by X is then equal to the sum $\bigoplus_{i\geq 1} E_i$ where E_i is the additive subgroup generated by the Lie monomials of degree i. E is the free Lie ring on X and $E_i = E \cap H_i$ (again, the Jacobi identity shows that E_i is spanned by the left-normed Lie monomials).

Given $f \in I^{(1)}$, we define $\exp(f)$ and $\log(1+f)$ by the classical series

$$\exp(f) = \sum_{n=0}^{\infty} \frac{f^n}{n!} \qquad \log(1+f) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{f^n}{n}$$

which are convergent in $\mathbb{Q}\langle\langle X\rangle\rangle$, and we have the familiar properties $\log\big(\exp(f)\big) = f$ and $\exp\big(\log(1+f)\big) = 1+f$. It follows that if $f, g \in I^{(1)}$ then there exists a unique element $h \in I^{(1)}$ with the property that $\exp(h) = \exp(f)\cdot\exp(g)$ and a formula for h is given by the Campbell–Hausdorff formula (it is not in general true that $h = f+g$). As Lazard [15] points out, this formula arose in the study of Lie groups and many names are associated with it, among them Poincaré, Schur, Baker, Dynkin and Pascal, to name but a few. The standard reference for this formula seems to be Jacobson [11] and we follow his lead in referring to it as the Campbell–Hausdorff formula.

In [11], the problem of finding an expression for h is done in the situation when $X = \{x, y\}$ and f and g are taken to be x and y respectively. In this case, it is shown that h is an element of $\overline{L}$ and so is the limit of a series of elements of L — the Lie subalgebra of $\mathbb{Q}\langle\langle X\rangle\rangle_L$ generated by X — and, using this fact, this series is obtained explicitly with each term of the series being a rational multiple of a left-normed Lie monomial in x and y. This series is denoted by $\Phi(x, y)$ and is called the ***Campbell–Hausdorff formula***. Up to degree 3, the formula is given by

$$\Phi(x,y) = x + y + \frac{1}{2}[x,y] + \frac{1}{12}[x,y,y] - \frac{1}{12}[x,y,x] + \cdots \tag{1·2}$$

In order to establish the Lie ring correspondence which we require, we will not need the full expression for $\Phi(x, y)$ and so will not reproduce it here (it can be found on p.173 of [11]). We will however, need a fact about the denominators which occur in the coefficients of the terms of the series. Specifically, for any $i \geq 1$, the denominator of the coefficient of a term of degree i is divisible only by those primes which are less than or equal to i. So in particular (and this is the principal fact which we will use), if p is a prime number then the denominator of the coefficient of a term of degree less than p is invertible modulo any power of p.

The above formula can now be applied to the general situation where X is an arbitrary finite set of symbols and $f, g \in I^{(1)}$ to obtain an expression for $\log\big(\exp(f)\cdot\exp(g)\big)$ by observing that, denoting the associative subalgebra generated by f and g by $\langle f, g\rangle$, there is a continuous $\mathbb{Q}$-algebra homomorphism

$$s : I^{(1)}\big(\mathbb{Q}\langle\langle\{x,y\}\rangle\rangle\big) \longrightarrow \overline{\langle f, g\rangle} \tag{1·3}$$

where the image of an element of $\mathbb{Q}\langle\langle x, y\rangle\rangle$ is the limit of the series obtained by substituting f for x and g for y (this limit exists by completeness since $f, g \in I^{(1)}$ guarantees that the terms of the series tend to zero). It then follows that $\log\big(\exp(f)\cdot\exp(g)\big) = s\big(\Phi(x,y)\big) = \Phi(f,g)$.

We can now use the Campbell–Hausdorff formula to define a multiplication $*$ on $I^{(1)}$ by defining the product of two elements $f, g \in I^{(1)}$ by

$$f * g = \Phi(f,g).$$

This multiplication is associative since if $f, g, h \in I^{(1)}$ then

$$\begin{aligned}\Phi\big(\Phi(f,g),h\big) = \log\big((\exp(f)\cdot\exp(g))\cdot\exp(h)\big) &= \log\big(\exp(f)\cdot(\exp(g)\cdot\exp(h))\big)\\ &= \Phi\big(f,\Phi(g,h)\big)\end{aligned}$$

Also, it follows from (1·2) that $\Phi(f,0) = \Phi(0,f) = 0$ and $\Phi(f,-f) = \Phi(-f,f) = 0$, so that $I^{(1)}$ equipped with the product $*$ is a group. To avoid possible confusion with the Lie bracket on $I^{(1)}$, we will denote the group commutator of $f, g \in I^{(1)}$ by (f,g), and from (1·2) we can see that

$$(f,g) = [f,g] + \frac{1}{2}[f,g,f] + \frac{1}{2}[f,g,g] + \text{ terms of order } \geq 4 \qquad (1\cdot4)$$

Using (1·2) it is straightforward to see that the metric induced on $(I^{(1)}, *)$ from $\mathbb{Q}\langle\langle X\rangle\rangle$ yields a complete topological group, and in this group the subgroup generated by X is of principal importance, mainly because it is a free group on this set. To see why this is the case we first need to introduce the complex commutators in a free group (in the same way that we introduced the general Lie monomials). So let $F = F(X)$ denote the free group on X and define a function $\sigma : \cup_{i\geq 1} X_i \to F$ inductively by setting $\sigma(x) = x$ for $x \in X_1$, and then if (u,v) is a non-associative word of degree $i > 1$ we set $\sigma\big((u,v)\big)$ to be the group commutator $\big(\sigma(u),\sigma(v)\big)$ of $\sigma(u)$ and $\sigma(v)$ in $F(X)$. The elements $\sigma(X_i)$ are referred to as the complex commutators in X of weight i and since the lower central series is strongly central we have $\sigma(X_i) \subseteq \gamma_i(F)$ for any $i \geq 1$ ($\gamma_i(F)$ is the i^{th} term of the lower central series of F). Magnus [17], [18] and Witt [31] studied the lower central series of free groups and established a connection between complex commutators and Lie monomials which we will

need. If for $i \geq 1$ we denote by π_i and σ_i the restriction to X_i of the maps $\pi : \cup_{j\geq 1} X_j \to E$ and $\sigma : \cup_{j\geq 1} X_j \to F$ (E is the free Lie ring on X as in the previous note) respectively, then they showed that there exists a (unique) isomorphism ρ_i of Abelian groups which makes the following diagram commute

$$\begin{array}{ccccc} X_i & \xrightarrow{\sigma_i} & \gamma_i(F) & \xrightarrow{\text{nat}} & \gamma_i(F)/\gamma_{i+1}(F) \\ & \searrow^{\pi_i} & & \swarrow_{\rho_i} & \\ & & E_i & & \end{array}$$

In addition, for any $i, j \geq 1$ with $a \in \gamma_i(F)$ and $b \in \gamma_j(F)$ we have

$$\rho_{i+j}\big((a,b)\,\gamma_{i+j+1}(F)\big) = \big[\rho_i\big(a\,\gamma_{i+1}(F)\big), \rho_j\big(b\,\gamma_{j+1}(F)\big)\big].$$

Now since E_i is a subgroup of a free Abelian group (namely the additive subgroup of $\mathbb{Q}\langle X\rangle$ with basis the associative monomials of degree i) it is also a free Abelian group and if we have a $\mathbb{Z}-$basis of E_i consisting of Lie monomials of degree i then the corresponding complex commutators form a $\mathbb{Z}-$basis of $\gamma_i(F)/\gamma_{i+1}(F)$ by the above isomorphism. M. Hall Jr. [5] gave an inductive procedure for finding such a $\mathbb{Z}-$basis of each E_i and the elements which arise (called standard Lie monomials) correspond (under the above isomorphism) to the commutators which arise in P. Hall's collecting process in [7].

If we now let G be the subgroup of $(I^{(1)}, *)$ generated by X and denote by θ the group homomorphism $F(X) \to G$ which extends the identity map on X, then the following lemma follows by a simple inductive argument using (1·4) and the above remarks

Lemma 1·1. *Let $i \geq 1$ and suppose that $w \in X_i$ with $\sigma_i(w) \in \gamma_i(F) \setminus \gamma_{i+1}(F)$. Then $\theta(\sigma_i(w))$ has order i and $h_i\big(\theta(\sigma_i(w))\big) = \pi_i(w)$.*

Using this lemma and the fact that each $\gamma_i(F)/\gamma_{i+1}(F)$ is free Abelian and possesses a basis of (images of) complex commutators, we obtain the following.

Lemma 1·2. *If $i \geq 1$ and $a \in \gamma_i(F) \setminus \gamma_{i+1}(F)$ then $\theta(a)$ has order i and $h_i\big(\theta(a)\big) = \rho_i\big(a\gamma_{i+1}(F)\big)$.*

This lemma then implies that for each $i \geq 1$ we have $G \cap I^{(i)} = \gamma_i(G)$ and so using the theorem of Magnus that the terms of the lower central series of a free group have trivial

intersection (see e.g. [10]), it follows that the kernel of θ must be trivial so that θ is in fact an isomorphism and G is therefore free on X. Moreover, if we define a metric on $F(X)$ by defining the ball of radius 2^{-i} around an element u to be the coset $u\,\gamma_i(F)$, then $F(X)$ becomes a topological group with θ giving an isometric embedding of $F(X)$ in $(I^{(1)}, *)$ (using the fact that for $g, h \in I^{(1)}$ we have $g^{-1} * h \in I^{(i)}$ if and only if $-g + h \in I^{(i)}$), and since the latter is complete, the closure $\overline{G}$ of G is a completion of $F(X)$. Also, since G is contained in $\overline{L}$ it follows that $\overline{G} \subseteq \overline{L}$.

We now consider the question of how to express the sum $f + g$ and Lie bracket $[f, g]$ of two arbitrary elements $f, g \in I^{(1)}$ in terms of the group operation $*$ on $I^{(1)}$ — this is what Lazard [15] calls "inversion" of the Campbell-Hausdorff formula. In order to achieve this we need to introduce fractional exponents and infinite products in $(I^{(1)}, *)$. Given an element f of $I^{(1)}$ and integers r, s with s non-zero, we wish to define $f^{\frac{r}{s}}$ to be an element g where $g^s = f^r$ and so since f^r (f raised to the power r in the group $(I^{(1)}, *)$) equals rf (this follows immediately from the definition of $*$), g must be defined to be $\frac{r}{s}f$. With this definition of fractional exponents the following properties are straightforward for any $f \in I^{(1)}$ and $\lambda, \mu \in \mathbb{Q}$

$$f^{\lambda+\mu} = f^{\lambda} * f^{\mu} \quad \text{and} \quad (f^{\lambda})^{\mu} = f^{\lambda\mu}.$$

Given a sequence $(f_n)_{n\in\mathbb{N}}$ of elements of $I^{(1)}$ we say that the infinite (ordered) product $\prod_{n\in\mathbb{N}} f_n$ converges if the sequence of finite products $(\prod_{n=1}^{k} f_n)_{k\in\mathbb{N}}$ converges, and by completeness this is equivalent to saying that the sequence (f_n) tends to zero.

The general inversion question will follow from a consideration of the inversion question restricted to $\overline{L}$, and so we address this situation first (recalling that an element $f \in I^{(1)}(\mathbb{Q}\langle\langle X\rangle\rangle)$ belongs to $\overline{L}$ if and only if for each $i \geq 1$, $h_i(f) \in K_i$).

For each $i \geq 1$ we choose a $\mathbb{Z}-$basis $B_i = \{b_{i,1}, \ldots, b_{i,d_i}\}$ of E_i which consists of Lie monomials of degree i (for instance by following the procedure of Hall [5]), and then, identifying the free group $F(X)$ with G, we denote by $C_i = \{c_{i,1}, \ldots, c_{i,d_i}\}$ the complex commutators of degree i which "correspond" to the respective elements of B_i via the above commutative diagram so that for any $i \geq 1$ with $1 \leq j \leq d_i$ we have $h_i(c_{i,j}) = b_{i,j}$, i.e. $c_{i,j} = b_{i,j} + e_{i,j}$ where $\omega(e_{i,j}) \geq i + 1$. Observe also that since each Lie monomial of degree i is a $\mathbb{Z}-$linear combination of the elements of B_i it follows that B_i is a $\mathbb{Q}-$basis of the

$\mathbb{Q}$−vector space K_i spanned by the Lie monomials of degree i. The following theorem (and its proof) enables us to give an effective procedure for calculating the inversion formulas.

Theorem 1·3. (Lazard [15]) *Let f be an element of $\overline{L}$. Then there exists a set of rational numbers $\{\lambda_{i,j} : i \in \mathbb{N}, 1 \leq j \leq d_i\}$, uniquely determined by f, and such that*

$$f = \prod_{i=1}^{\infty} z_i \quad \text{where} \quad z_i = \prod_{j=1}^{d_i} c_{i,j}^{\lambda_{i,j}} \quad \text{for each } i \in \mathbb{N}.$$

Proof. ([15]) Firstly, observe that for any $i \geq 1$ and rationals $\lambda_{i,1}, \ldots, \lambda_{i,d_i}$ we have

$$\prod_{j=1}^{d_i} c_{i,j}^{\lambda_{i,j}} = \sum_{j=1}^{d_i} \lambda_{i,j} b_{i,j} + \text{terms of order } > i$$

with this product belonging to $\overline{L} \cap I^{(i)}$, and so if f is the limit of a product $\prod_i z_i$ as in the statement, then for any $k \geq 1$ we must have

$$z_{k-1}^{-1} \cdots z_1^{-1} f = \prod_{i=k}^{\infty} z_i \in \overline{L} \cap I^{(k)}.$$

With this observation, we show how to inductively calculate the z_i. So suppose that $k \geq 1$ and we have calculated elements $z_1, \ldots, z_{k-1}$ of $\overline{L}$ with the property that for any i with $1 \leq i \leq k-1$ we have $z_i^{-1} \cdots z_1^{-1} f \in \overline{L} \cap I^{(i+1)}$. So in particular, $z_{k-1}^{-1} \cdots z_1^{-1} f \in \overline{L} \cap I^{(k)}$ from which it follows that

$$z_{k-1}^{-1} \cdots z_1^{-1} f = h_k(z_{k-1}^{-1} \cdots z_1^{-1} f) + r,$$

where $\omega(r) \geq k+1$ and $h_k(z_{k-1}^{-1} \cdots z_1^{-1} f) \in K_k$ (since $z_{k-1}^{-1} \cdots z_1^{-1} f \in \overline{L}$). Therefore, there exist rationals $\lambda_{k,1}, \ldots, \lambda_{k,d_k}$ such that

$$h_k(z_{k-1}^{-1} \cdots z_1^{-1} f) = \sum_{j=1}^{d_k} \lambda_{k,j} b_{k,j},$$

and so since

$$\prod_{j=1}^{d_k} c_{k,j}^{\lambda_{k,j}} = \sum_{j=1}^{d_k} \lambda_{k,j} b_{k,j} + s$$

with $\omega(s) \geq k+1$, it follows that

$$\Big(\prod_{j=1}^{d_k} c_{k,j}^{\lambda_{k,j}}\Big)^{-1} z_{k-1}^{-1} \cdots z_1^{-1} f \;=\; r - s \;\in\; \overline{L} \cap I^{(k+1)}.$$

Hence we set $z_k = \prod_{j=1}^{d_k} c_{k,j}^{\lambda_{k,j}}$, and therefore by induction we have a sequence $(z_i)_{i \in \mathbf{N}}$ of elements of $\overline{L}$ where for any $k \in \mathbf{N}$, $z_k^{-1} \cdots z_1^{-1} f \in \overline{L} \cap I^{(k+1)}$, from which it follows that $f = \prod_i z_i$. The fact that f determines the $\lambda_{i,j}$ is evident from the construction since each B_i forms a $\mathbf{Q}-$basis of K_i. $\square$

Note. The proof gives a procedure for calculating z_k provided that B_k is known, and we know $z_1, \ldots, z_{k-1}, f$, and (1·2) up to and including degree k.

By restricting the elements f which are considered it is possible to obtain more information about the rational exponents which appear in the above procedure. In particular, we obtain Lazard's inversion formulas by restricting attention to a certain closed Lie subring $M = M(X)$ of $\overline{L}$ which is also a subgroup of $(\overline{L}, *)$ containing G. Specifically, if for each $i \geq 1$ we denote by $\mathbf{Z}[1/i!]$ the subring of $\mathbf{Q}$ consisting of those rationals which, in lowest terms, have denominator divisible only by primes less than or equal to i, then M is taken to be the set of elements f of $\overline{L}$ in which for any $i \geq 1$, $h_i(f)$ is expressible as a $\mathbf{Z}[1/i!]-$linear combination of Lie monomials of degree i. It follows immediately from the definition that M is a closed Lie subring of $\overline{L}$; the fact that M is a subgroup of $(\overline{L}, *)$ follows by applying the aforementioned important property of the Campbell–Hausdorff formula that the coefficient of any term of degree i in (1·2) belongs to $\mathbf{Z}[1/i!]$, and since $X \subseteq M$ we see that M contains G. Restricting attention to M we have the following result

Theorem 1·4. ([15] 2.7.) *Let f be an element of M and suppose that $f = \prod_i z_i$ with $z_i = \prod_{j=1}^{d_i} c_{i,j}^{\lambda_{i,j}}$, as asserted by theorem 1·3. Then for any $i \geq 1$ we have $\lambda_{i,1}, \ldots, \lambda_{i,d_i} \in \mathbf{Z}[1/i!]$.*

Proof. Suppose that $k \geq 1$ and that the theorem is true for $1 \leq i \leq k-1$ (for induction). So we know that $z_1, \ldots, z_{k-1} \in M$ and therefore $z_{k-1}^{-1} \cdots z_1^{-1} f \in M$. Now by the proof of

theorem 1·3 we know that

$$\sum_{j=1}^{d_k} \lambda_{k,j}\, b_{k,j} = h_k(z_k^{-1} \cdots z_1^{-1} f),$$

and so it follows from the definition of M that $\sum_{j=1}^{d_k} \lambda_{k,j}\, b_{k,j}$ is a $\mathbb{Z}\big[1/k!\big]-$linear combination of Lie monomials of degree k. We therefore must have $\lambda_{k,1}, \ldots, \lambda_{k,d_k} \in \mathbb{Z}\big[1/k!\big]$. □

We now use theorems 1·3 and 1·4 to derive Lazard's inversion formulas. Suppose first that $X = \{x, y\}$ so that the elements of C_i are complex commutators of weight i in x and y. Then since $x + y$ and $[x, y]$ belong to $M\big(\{x, y\}\big)$, theorems 1·3 and 1·4 assert the existence of two sets of rationals $\big\{\lambda_{i,j} : i \in \mathbb{N}, 1 \leq j \leq d_i\big\}$ and $\big\{\mu_{i,j} : i \in \mathbb{N}, 1 \leq j \leq d_i\big\}$, such that

$$x + y = \prod_{i=1}^{\infty}\Big(\prod_{j=1}^{d_i} c_{i,j}^{\lambda_{i,j}}\Big) \qquad\qquad [x, y] = \prod_{i=1}^{\infty}\Big(\prod_{j=1}^{d_i} c_{i,j}^{\mu_{i,j}}\Big) \tag{1·5}$$

and

$$\begin{gathered}\lambda_{i,1}, \ldots, \lambda_{i,d_i} \in \mathbb{Z}\big[1/i!\big] \\ \text{for each } i \in \mathbb{N}\end{gathered} \qquad\qquad \begin{gathered}\mu_{i,1}, \ldots, \mu_{i,d_i} \in \mathbb{Z}\big[1/i!\big] \\ \text{for each } i \in \mathbb{N}\end{gathered} \tag{1·6}$$

(1·5) and (1·6) are Lazard's inversion formulas. Using the fact that (1·2) gives the terms of the Campbell–Hausdorff formula up to degree 3, and by taking $B_1 = \{x, y\}$, $C_1 = \{x, y\}$, $B_2 = \big\{[x, y]\big\}$, $C_2 = \big\{(x, y)\big\}$, $B_3 = \big\{[x, y, x], [x, y, y]\big\}$, $C_3 = \big\{(x, y, x), (x, y, y)\big\}$, it is then straightforward to use the procedure of theorem 1·3 to obtain the following expansions of (1·5) up to degree 3

$$\begin{aligned} x + y &= x\, y\, (x, y)^{-\frac{1}{2}} (x, y, x)^{\frac{1}{12}} (x, y, y)^{-\frac{1}{12}} \cdots \\ [x, y] &= (x, y)(x, y, x)^{-\frac{1}{2}} (x, y, y)^{-\frac{1}{2}} \cdots \end{aligned} \tag{1·7}$$

We can now apply (1·5) and (1·6) to the general situation where X is an arbitrary finite set of symbols and we wish to express the sum $f + g$ and the Lie bracket $[f, g]$ of two arbitrary elements $f, g \in I^{(1)}(\mathbb{Q}\langle\langle X \rangle\rangle)$ in terms of the group operation on $I^{(1)}$. To do this,

we consider the continuous $\mathbb{Q}-$algebra homomorphism $s : I^1(\mathbb{Q}\langle\langle\{x,y\}\rangle\rangle) \to \overline{\langle f,g\rangle}$, as in (1·3), and observe that by the Campbell–Hausdorff formula, s gives a continuous group homomorphism from $(I^{(1)}(\mathbb{Q}\langle\langle\{x,y\}\rangle\rangle),*)$ to $(I^{(1)}(X),*)$ and so it follows that

$$f+g=\prod_{i=1}^{\infty}\Big(\prod_{j=1}^{d_i}s(c_{i,j})^{\lambda_{i,j}}\Big) \qquad \text{and} \qquad [f,g]=\prod_{i=1}^{\infty}\Big(\prod_{j=1}^{d_i}s(c_{i,j})^{\mu_{i,j}}\Big) \tag{1·8}$$

Section 1·1·3. The Functors $\mathcal{L}_p$ and $\mathcal{G}_p$.

In this section let p denote a fixed, but arbitrary, prime number. We now use Lazard's results presented in section 1·1·2 to indicate how he obtains the functors $\mathcal{L}_p$ and $\mathcal{G}_p$ between Λ_p, the category of finite nilpotent p-Lie rings U with $cl(U) < p$, and Γ_p, the category of finite p-groups P with $cl(P) < p$, as mentioned in section 1·1·1. We will continue to use the notation introduced in the previous section.

If U is an object of Λ_p then $1,2,\ldots,p-1$ act invertibly on U (regarded as a $\mathbb{Z}-$module), and so U can also be thought of as a $\mathbb{Z}\big[1/(p-1)!\big]-$Lie algebra. Now, if x and y are any two elements of U then any Lie monomial of degree at least p in x and y will vanish in U (since $cl(U) < p$), and so the formula $\Phi(x,y)$ given by (1·2) makes sense in U since all terms of degree less than p have coefficients belonging to $\mathbb{Z}\big[1/(p-1)!\big]$. We therefore define the product $x*y$ of x and y to be the element of U given by $\Phi(x,y)$ and denote $(U,*)$ by $\mathcal{G}_p(U)$ (observe that U and $\mathcal{G}_p(U)$ have the same underlying set). To see that $\mathcal{G}_p(U)$ is a group, we choose a suitable set X so that the free Lie ring $E(X)$ maps onto U and then, regarding $E(X)$ as a Lie subring of $\mathbb{Q}\langle\langle X\rangle\rangle_L$ (as in the previous section), Lazard [15] showed that this mapping can be extended to a Lie ring homomorphism $\tau : M(X) \to U$, where for $i \geq p$ we have $I^{(i)} \cap M(X) \subseteq \ker\tau$. Then, if $x,y \in U$ and $f,g \in M(X)$ are chosen so that $\tau(f) = x$ and $\tau(g) = y$, it follows that $\tau\big(\Phi(f,g)\big) = x*y$, and so since $M(X)$ equipped with the Campbell–Hausdorff product is a group, we see that $\mathcal{G}_p(U)$ is a group with τ giving a group homomorphism from $M(X)$ onto $\mathcal{G}_p(U)$. Also, by (1·4) we see that the p^{th}-term of the lower central series of the group $(M(X),*)$ is contained in $I^{(p)} \cap M(X)$, and so it follows that the $p^{\text{th}}-$term of the lower central series of $\mathcal{G}_p(U)$ vanishes so that $cl(\mathcal{G}_p(U)) < p$. Therefore $\mathcal{G}_p(U)$ is an object of Γ_p. If V is another object

of Λ_p and $\phi \in \mathrm{Hom}(U,V)$, then it follows from the Campbell–Hausdorff formula (1·2) that $\phi \in \mathrm{Hom}\big(\mathcal{G}_p(U),\mathcal{G}_p(V)\big)$, and so setting $\mathcal{G}_p(\phi)$ to be ϕ we see that $\mathcal{G}_p$ gives a covariant functor between Λ_p and Γ_p.

In order to introduce the functor $\mathcal{L}_p$ we first need some terminology. Letting S be a set of prime numbers and $n \in \mathbb{N}$ we will write $n \mid S$ if n is divisible only by primes which are contained in S. If H is then an arbitrary group we say that H is ***S–divisible*** if $x \in H$ and $n \mid S$ implies the existence of an element $y \in H$ with $y^n = x$; we say that H is ***without S–torsion*** if $x \in H$ with $x^n = 1$ and $n \mid S$ implies that $x = 1$. If we let P be a finite p-group and S a set of primes such that $p \notin S$, then using the fact that each quotient $\gamma_i(P)/\gamma_{i+1}(P)$ is S–divisible and without S–torsion, it is straightforward to show that any element x of P has a **unique** n^{th}–root (where $n \mid S$). In particular, this holds when P is an object of Γ_p and we take S to be the set of primes less than p. In this case, for any element x of P and $\lambda \in \mathbb{Z}\big[1/(p-1)!\big]$ we can unambiguously define x^λ to be the element $(x^r)^{1/s}$ (where $\lambda = r/s$ in lowest terms) so that

$$x^{\lambda+\mu} = x^\lambda x^\mu \quad \text{and} \quad x^{\lambda\mu} = (x^\lambda)^\mu \quad \text{for any} \quad \lambda,\mu \in \mathbb{Z}\big[1/(p-1)!\big].$$

So, if P is an object of Γ_p and $x,y \in P$ then it follows (by equation (1·6) and the fact that $cl(P) < p$), that the formulas given by equation (1·5) make sense in P. We therefore use equation (1·5) to define the sum $x + y$ and bracket $[x,y]$ of $x,y \in P$, and denote P equipped with these two operations by $\mathcal{L}_p(P)$. To see that $\mathcal{L}_p(P)$ is a Lie ring we choose a suitable set X such that the free group $F(X)$ maps onto P and then, regarding $F(X)$ as the subgroup G of $I^{(1)}(\mathbb{Q}\langle\langle X\rangle\rangle)$ (as defined in the previous section), Lazard showed ([15] Ch. 2. §3) that this mapping can be extended to a group homomorphism $\psi : M(X) \to P$ where for $i \geq p$ we have $I^{(i)} \cap M(X) \subseteq \ker\psi$. To see that $\mathcal{L}_p(P)$ is a Lie ring we observe that if $x,y \in P$ and $f,g \in M(X)$ are chosen so that $\psi(f) = x$ and $\psi(g) = y$, then using the formulas given in (1·8) it follows that $\psi(f+g) = x + y$ and $\psi\big([f,g]\big) = [x,y]$. From this, we see that $\mathcal{L}_p(P)$ is a Lie ring and ψ then gives a Lie ring homomorphism from $M(X)$ onto $\mathcal{L}_p(P)$. Also, since the p^{th}–term of the lower central series of the Lie ring $M(X)$ is contained in $I^{(p)} \cap M(X)$ it follows that $\mathcal{L}_p(P)$ is nilpotent with $cl\big(\mathcal{L}_p(P)\big) < p$. If Q is another object of Γ_p and $\theta \in \mathrm{Hom}(P,Q)$ then it follows that $\theta \in \mathrm{Hom}\big(\mathcal{L}_p(P),\mathcal{L}_p(Q)\big)$

by using equation (1·5) and the fact that for any $x \in P$, and $\lambda \in \mathbb{Z}\left[1/(p-1)!\right]$ we have $\theta(x^\lambda) = \theta(x)^\lambda$. So setting $\mathcal{L}_p(\theta)$ to be θ we see that $\mathcal{L}_p$ is a covariant functor from Γ_p to Λ_p.

From the fact that equation (1·5) gives us the Lie operations on $M(X)$ in terms of the group structure, it follows that (1·5) can be used to recover the Lie structure on U from the group structure on $\mathcal{G}_p(U)$, and since this is the method used to obtain the Lie ring $\mathcal{L}_p(\mathcal{G}_p(U))$ it follows that this is the same Lie ring as U. Similarly, equation (1·2) gives the group structure on $M(X)$ in terms of the Lie operations on $M(X)$, and so the group structure on P can be recovered from $\mathcal{L}_p(P)$ by using (1·2). Hence P and $\mathcal{L}_p(\mathcal{G}_p(P))$ are the same group.

To summarise the above, we have the following result.

Theorem 1·5. (Magnus [19], Lazard [15]) *$\mathcal{L}_p$ and $\mathcal{G}_p$ give mutually inverse isomorphisms between the categories Γ_p and Λ_p.*

As well as preserving underlying sets, $\mathcal{L}_p$ and $\mathcal{G}_p$ also preserve certain structural properties which we now summarise, so let P be an arbitrary object of Γ_p where we denote group multiplication by juxtaposition which, by theorem 1·5, coincides with the Campbell–Hausdorff product on $\mathcal{L}_p(P)$.

Using (1·2) we see that the multiplicative identity of P coincides with the additive identity of $\mathcal{L}_p(P)$ and also that if $x \in P$ and $n \in \mathbb{N}$ then $x^n = nx$ so that the multiplicative order of an element is equal to its additive order. It therefore follows that the exponent of P equals the additive exponent of the Abelian p-group $(\mathcal{L}_p(P), +)$. We also see that if $n \mid S$ (where S is the set of primes less than p) then $(\frac{1}{n}x)^n = x$ so that by uniqueness of n^{th}–roots we have $\frac{1}{n}x = x^{\frac{1}{n}}$, and therefore for any element $\lambda \in \mathbb{Z}\left[1/(p-1)!\right]$ we have $\lambda x = x^\lambda$.

If H is a subgroup of P then for any $x \in H$ and $\lambda \in \mathbb{Z}\left[1/(p-1)!\right]$, $x^\lambda \in H$ (this follows by uniqueness of roots), and so by (1·5) we see that H is also a subring of $\mathcal{L}_p(P)$. Similarly, if H is a subring of $\mathcal{L}_p(P)$ then H is also a Lie sub-algebra of $\mathcal{L}_p(P)$ regarded as a $\mathbb{Z}\left[1/(p-1)!\right]$–Lie algebra, and so by (1·2) we see that H is also a subgroup of P. Hence the lattice of subgroups of P coincides with the lattice of subrings of $\mathcal{L}_p(P)$. Moreover, if

N is a ***normal*** subgroup of P then we see that N is also an ideal of $\mathcal{L}_p(P)$, and vice-versa, so that the lattice of normal subgroups of P coincides with the lattice of ideals of $\mathcal{L}_p(P)$. Further, if N is a normal subgroup of P then for any element x of P we see from (1·2) and (1·5) that $xN = x + N$, so that the multiplicative cosets of N coincide with the additive cosets of N. Hence the quotient group P/N and the quotient ring $\mathcal{L}_p(P)/N$ are the same set. But we also know that P/N is in Γ_p and $\mathcal{L}_p(P)/N$ is in Λ_p, and so denoting the Campbell-Hausdorff product on $\mathcal{L}_p(P)/N$ by $*$, we have, for any $x, y \in P$,

$$(x + N) * (y + N) = \Phi(x + N, y + N) = \Phi(x, y) + N = xy + N = xyN = (xN)(yN).$$

Hence, we see that $P/N = \mathcal{G}_p(\mathcal{L}_p(P)/N)$, or equivalently, $\mathcal{L}_p(P/N) = \mathcal{L}_p(P)/N$. Summarising this, we have

Lemma 1·6. *If P is in Γ_p and N is a normal subgroup of P then N is an ideal of $\mathcal{L}_p(P)$ and $\mathcal{L}_p(P/N) = \mathcal{L}_p(P)/N$.*

We now consider the relationship between central series of P and central series of $\mathcal{L}_p(P)$. First, observe that if H and J are normal subgroups of P then by equation (1·4) we see that the commutator group (H, J) is contained is the Lie subring $[H, J]$ of $\mathcal{L}_p(P)$, and vice-versa (by (1·5)), so that we have $(H, J) = [H, J]$. A simple induction then shows that the i^{th}−term $\gamma_i(P)$ of the lower central series of P coincides with the i^{th}−term $\gamma_i(\mathcal{L}_p(P))$ of the lower central series of $\mathcal{L}_p(P)$, so that, in particular, P and $\mathcal{L}_p(P)$ have the same nilpotency class. More generally, if $P = N_1 \geq N_2 \geq \cdots$ is any descending series of normal subgroups of P, then such a series is a central series of P if and only if it is a central series of $\mathcal{L}_p(P)$.

If $x, y \in P$ then from equations (1·4) and (1·5) it follows that the group commutator (x, y) equals 1 if and only if the Lie bracket $[x, y]$ equals 0, so that the centralisers

$$C_P(x) = \{y \in P : (x, y) = 1\} \text{ and } C_{\mathcal{L}_p(P)}(x) = \{y \in \mathcal{L}_p(P)\} : [x, y] = 0\}$$

coincide. In particular, it follows that the centre $Z(P)$ of P coincides with the centre $Z(\mathcal{L}_p(P))$ of $\mathcal{L}_p(P)$.

The above remarks give a good indication that, in addition to being isomorphic categories, there is a strong structural connection between corresponding objects of Γ_p and Λ_p. Therefore, if we are interested in questions involving only the properties which are preserved, then it is possible to recast a question about p-groups in Γ_p in terms of Lie rings in Λ_p. If the resulting question can be solved, then the solution to the original problem can be recovered by using the functorial correspondence. We will make use of this approach.

Section 1·2. Regular p-Groups.

Throughout, let p denote a fixed, but arbitrary, prime number. In this section we collate the various results which we will need concerning regular p-groups.

Given a finite p-group P and a non-negative integer i, define two subgroups $\Omega_i(P)$ and $\mathfrak{U}_i(P)$ by

$$\Omega_i(P) = \langle x : x^{p^i} = 1 \rangle$$

$$\mathfrak{U}_i(P) = \langle x^{p^i} : x \in P \rangle.$$

This gives an ascending series

$$1 = \Omega_0(P) \leq \Omega_1(P) \leq \Omega_2(P) \leq \cdots$$

and a descending series

$$P = \mathfrak{U}_0(P) \geq \mathfrak{U}_1(P) \geq \mathfrak{U}_2(P) \geq \cdots$$

of fully invariant subgroups of P which are called the $\Omega-$ and $\mathfrak{U}-$ series respectively. P is called **regular** if, given any two elements x, y of P it is possible to find an element c of $\mathfrak{U}_1(\gamma_2(\langle x, y \rangle))$ satisfying

$$x^p y^p = (xy)^p c.$$

The notion of regularity was introduced by Phillip Hall in [7] and is considered in some detail. Several results draw an analogy between the "order-power" structure of a regular p-group P and that of an Abelian p-group. These results are summarised in the following theorem

Theorem 1·7. (Hall [7]) *Let P be a finite regular p-group. Then*

i) Given any two elements x, y of P and a non-negative integer i, $x^{p^i} = y^{p^i}$ if and only if $(x^{-1}y)^{p^i} = 1$.

ii) $\Omega_i(P)$ is precisely the set of elements of P whose order is at most p^i.

iii) $\mathfrak{U}_i(P)$ is precisely the set of p^i-th powers of elements of P.

iv) $|P : \Omega_i(P)| = |\mathfrak{U}_i(P)|$ for any i.

Using part i) of theorem 1·7 it is straightforward to obtain the following corollary.

Corollary 1·8. *Let P be a finite regular p-group. Given any two elements x, y of P and non-negative integers i, j, we have*

$$[x^{p^i}, y^{p^j}] = 1 \text{ if and only if } [x,y]^{p^{i+j}} = 1.$$

In [7], Hall introduced his collecting process and used it to show that if we fix a natural number n, then in the free group $F = F(\{x,y\})$ there exist elements $c_2, \ldots, c_n$ with $c_i \in \gamma_i(F)$ for each $i = 2, \ldots, n$, such that

$$x^n y^n = (xy)^n c_2^{e_2} \cdots c_n^{e_n} \tag{1·9}$$

where e_i is the i^{th} binomial coefficient $(2 \leq i \leq n)$. If we now let P be a finite p-group of nilpotency class less than p and consider two elements g, h of P with the homomorphism θ from the free group $F = F(\{x,y\})$ onto $\langle g, h\rangle$ where $\theta(x) = g$ and $\theta(y) = h$, then using equation (1·9) we see that

$$g^p h^p = (gh)^p \theta(c_2)^{e_2} \cdots \theta(c_{p-1})^{e_{p-1}}$$

(since $cl(P) < p$ implies that $\gamma_p(F) \subseteq \ker\theta$). Therefore, since p divides $e_2, \ldots, e_{p-1}$ it follows that $\theta(c_2)^{e_2} \cdots \theta(c_{p-1})^{e_{p-1}}$ is an element of $\mathfrak{U}_1(\gamma_2(\langle g,h\rangle))$, and so we have the following important result

Theorem 1·9. ([7] 4.13.) *If P is a finite p-group of nilpotency class less than p, then P is regular.*

P. Hall investigated the idea of regularity further in [8] and gave a useful criterion for a finite p-group to be regular which we will need later. If, for an arbitrary finite p-group P, we define the invariant $\omega = \omega(P)$ by

$$p^{\omega(P)} = |P : \mathfrak{U}_1(P)|,$$

then P is called **absolutely regular** if $\omega(P) < p$. P. Hall showed the following result

Proposition 1·10. ([8]) *If P is absolutely regular then P is regular.*

We will be applying this result later to particular p-groups which have large cyclic subgroups in order to deduce that regularity automatically holds.

Given a sequence $B = (y_1, \ldots, y_k)$ of distinct non-identity elements of a p-group P with corresponding orders $(p^{e_1}, \ldots, p^{e_k})$ we recall the following definitions (from [7]).

Definition 1. *B is called a* **Uniqueness Basis** *(U.B.) of P if any element x of P is uniquely expressible in the form*

$$x = y_1^{f_1} y_2^{f_2} \ldots y_k^{f_k} \text{ where } 0 \leq f_i < p^{e_i} \text{ for each } i = 1, \ldots, k.$$

Definition 2. *B is called a* **Canonical Basis** *(C.B.) of P if the following two conditions are satisfied*

i) There exists a chain $P = Q_0 \triangleright Q_1 \triangleright \ldots \triangleright Q_k = \mathfrak{U}_1(P)$ of normal subgroups of P such that for each $i = 0, \cdots, k-1$, $|Q_i : Q_{i+1}| = p$ and $Q_i \setminus Q_{i+1}$ contains exactly one element of B.

ii) The product $\prod_{i=1}^{k} p^{e_i}$ is minimal subject to condition i) holding.

The fact that any p-group P possesses a C.B. is immediate from the definition and P. Hall observed that these two definitions coincide for Abelian p-groups. P. Hall extended the analogy with Abelian p-groups by showing the following

Theorem 1·11. ([7] 4.53.) *If P is a finite regular p-group then any C.B. of P is a U.B. of P.*

Thus the family of p-groups which possess a U.B. includes the regular p-groups. In the theory of Abelian p-groups it is well-known that the orders corresponding to a U.B. are

invariants of the group and are called the type invariants of the group in question. P. Hall extended this notion of type invariants to include the regular p-groups which we now discuss.

Given a regular p-group P we define the invariant $\mu(P)$ (or simply μ when no confusion arises) by the condition that P has exponent $p^{\mu(P)}$ (by using theorem 1·7 it is easy to see that $\mu(P)$ is the length of the $\Omega-$ or $\mathfrak{U}-$ series of P), and for $1 \leq i \leq \mu$ we define $\omega_i = \omega_i(P)$ by

$$p^{\omega_i} = |\Omega_i(P)/\Omega_{i-1}(P)|.$$

$\omega_1, \ldots, \omega_\mu$ are called the **ω-invariants** of P, and we have the following result.

Theorem 1·12. ([7] 4.3.) *For each $i = 1, \ldots, \mu$ we have $p^{\omega_i} = |\mathfrak{U}_{i-1}(P)/\mathfrak{U}_i(P)|$, and furthermore $\omega_1 \geq \omega_2 \geq \cdots \geq \omega_\mu$.*

So for a regular p-group P, this theorem shows that $\omega_1(P)$ equals the invariant $\omega(P)$ defined above. Now using the $\omega-$invariants, we define the **type invariants** (or the **μ-invariants**) of a finite regular p-group P to be $\mu_1(P), \ldots, \mu_{\omega_1(P)}(P)$ (or simply $\mu_1, \ldots, \mu_{\omega_1}$ when no confusion arises), where for each $j = 1, \ldots, \omega_1$, we set μ_j to be the number of ω_i's with $\omega_i \geq j$. We then say that P is of *type* $(\mu_1, \mu_2, \ldots, \mu_{\omega_1})$. Observe that $\mu_1 = \mu$.

Theorem 1·13. ([7] 4.36.) *For each $i = 1, \ldots, \mu_1$, ω_i is the number of μ_j's with $\mu_j \geq i$ and if we let $|P| = p^n$ then we have $n = \sum_{i=1}^{\mu} \omega_i = \sum_{j=1}^{\omega_1} \mu_j$.*

The principal result concerning the type invariants of a regular p-group is the following :

Theorem 1·14. ([7] 4.51.) *Let P be a regular p-group of type$(\mu_1, \ldots, \mu_\omega)$ and with a U.B. $B = (y_1, \ldots, y_k)$. Then*

i) The orders of the elements of B are given in descending order of magnitude by $p^{\mu_1}, \ldots, p^{\mu_\omega}$ (and so $k = \omega$).

ii) If $x \in P$ factorises as $x = y_1^{r_1} \ldots y_k^{r_k}$ then $x \in \Omega_i(P)$ if and only if each of the factors $y_j^{r_j}$ belongs to $\Omega_i(P)$; and further, $x \in \mathfrak{U}_i(P)$ if and only if each of the factors $y_j^{r_j}$ does so.

Observe that if P is an Abelian p-group then it is automatically regular and by part i) of theorem 1·14 it follows that the above definition of type invariants coincides with the usual definition.

In Chapters 2 and 3 we will be concerned with investigating how the nilpotency class of a p-group is bounded by the logarithm to the base p of the index of a largest cyclic subgroup and we will need the following theorem

Theorem 1·15. ([7] 4.433.) *Let P be a regular p-group such that $\gamma_{\beta+1}(P) \subseteq \mho_\alpha(P)$ for some integers α, β. Then for any $k \geq 0$ we have $\gamma_{k\beta+1}(P) \subseteq \mho_{k\alpha}(P)$.*

In the later chapters we will be principally concerned with the regular p-groups which have nilpotency class less than p (i.e. the category Γ_p). If P is in Γ_p then P has an associated Abelian group structure which is the underlying Abelian group of the Lie ring $\mathcal{L}_p(P)$. Now, it is easy to see that the $\Omega-$ and $\mho-$ series of P coincide with the $\Omega-$ and $\mho-$ series of $(\mathcal{L}_p(P), +)$ respectively, and so it follows that the $\omega-$ invariants of P coincide with the $\omega-$invariants of $(\mathcal{L}_p(P), +)$. Hence we have the following result.

Lemma 1·16. *If P is in Γ_p then the type invariants of P coincide with the type invariants of the Abelian p-group $(\mathcal{L}_p(P), +)$.*

Also, if U is any finite (not necessarily nilpotent) p-Lie ring, then its underlying Abelian group is a (regular) p-group and it is easy to see that the $\mho-$ and $\Omega-$ series of U are ideals of U. We will say that U is of *type*$(\mu_1, \ldots, \mu_{\omega_1})$ if the Abelian p-group $(U, +)$ is of *type*$(\mu_1, \ldots, \mu_{\omega_1})$.

Section 1·3. An Application to Bases of Regular p-Groups.

In section 1·2 we presented certain results and ideas from P. Hall's classic paper [7] and saw, in particular, that associated to regular p-groups there are two notions of basis, canonical and uniqueness, which are related by the fact that any canonical basis of a regular p-group is also a uniqueness basis. A question which was left open (see p.92 of [7]) is whether a uniqueness basis of a regular p-group is necessarily a canonical basis, and in this section we will use a simple application of the Lie ring correspondence of section 1·1·3 to answer this question negatively by showing that if p is an odd prime and P is a p-group of exponent p and nilpotency class 2, then P possesses a uniqueness basis which is not a canonical basis (the Lie ring correspondence is applicable in this situation since P belongs to Γ_p). Since the basis we construct is also a basis of the underlying Abelian p-group of the Lie ring $\mathcal{L}_p(P)$, it is then natural to ask what connection there is between canonical and uniqueness bases of a regular p-group P in Γ_p, and bases of the corresponding Lie ring $\mathcal{L}_p(P)$. We will briefly consider this question. Throughout this chapter p will denote an arbitrary odd prime number.

In order to use the Lie ring correspondence to construct the required U.B. we first need to show how to express a product of powers of elements of a p-group P having exponent p and nilpotency class 2 in terms of the Lie operations on the corresponding Lie ring. This is the purpose of the following lemma where we use that fact that for such a group, the group operation is related to the Lie operations on $\mathcal{L}_p(P)$ by $xy = x + y + \frac{1}{2}[x,y]$ for any two elements x, y of P (recall the Campbell-Hausdorff formula (1·2)).

Lemma 1·17. *Let P be a p-group of exponent p and nilpotency class 2 and suppose that $x_1, x_2, \ldots$ is a sequence of elements of P. Define a sequence $y_1, y_2, \ldots$ of elements of $\mathcal{L}_p(P)$ by*

$$y_i = \sum_{j=1}^{i} x_j\,, \quad \text{for } i = 1\,, 2, \ldots$$

Then for $n \geq 2$ and integers $a_1, \ldots, a_n$ we have

$$y_1^{a_1} \cdots y_n^{a_n} = a_1 y_1 + \cdots + a_n y_n + \frac{1}{2} \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} \Big(\sum_{k=i}^{j-1} a_k\Big)\Big(\sum_{l=j}^{n} a_l\Big)\,[x_i, x_j].$$

Proof. We use induction on n.

For $n = 2$ we have

$$\begin{aligned} y_1^{a_1} y_2^{a_2} &= a_1 y_1 + a_2 y_2 + \frac{1}{2}[a_1 y_1, a_2 y_2] \\ &= a_1 y_1 + a_2 y_2 + \frac{1}{2}(a_1 a_2)[x_1, x_1 + x_2] \\ &= a_1 y_1 + a_2 y_2 + \frac{1}{2}(a_1 a_2)[x_1, x_2], \quad \text{as required.} \end{aligned}$$

Now suppose that $r > 2$ and the result is true for $n = r - 1$. Observe that

$$y_1^{a_1} \cdots y_r^{a_r} = y_1^{a_1} \cdots y_{r-1}^{a_{r-1}} + y_r^{a_r} + \frac{1}{2}\left[y_1^{a_1} \cdots y_{r-1}^{a_{r-1}}, y_r^{a_r} \right], \tag{1·10}$$

and by induction we see that $\frac{1}{2}\left[y_1^{a_1} \cdots y_{r-1}^{a_{r-1}}, y_r^{a_r} \right]$

$$= \frac{1}{2}\left[a_1 y_1 + \cdots + a_{r-1} y_{r-1} + \frac{1}{2} \sum_{i=1}^{r-2} \sum_{j=i+1}^{r-1} \left(\sum_{k=i}^{j-1} a_k \right) \left(\sum_{l=j}^{r-1} a_l \right) [x_i, x_j], a_r y_r \right]$$

$$= \frac{1}{2} a_r \left[a_1 y_1 + \cdots + a_{r-1} y_{r-1}, x_1 + \cdots + x_r \right] \quad \text{(since } \mathcal{L}(P) \text{ has nilpotency class 2)}$$

$$= \frac{1}{2} a_r \sum_{k=1}^{r-1} a_k \left[x_1 + \cdots + x_k, x_{k+1} + \cdots + x_r \right]$$

$$= \frac{1}{2} a_r \sum_{i=1}^{r-1} \sum_{j=i+1}^{r} \left(\sum_{k=i}^{j-1} a_k \right) [x_i, x_j].$$

So substituting this into (1·10) and using induction again we obtain

$$\begin{aligned} y_1^{a_1} \cdots y_r^{a_r} = a_1 y_1 + \cdots + a_r y_r &+ \frac{1}{2} \sum_{i=1}^{r-2} \sum_{j=i+1}^{r-1} \left(\sum_{k=i}^{j-1} a_k \right) \left(\sum_{l=j}^{r-1} a_l \right) [x_i, x_j] \\ &+ \frac{1}{2} a_r \sum_{i=1}^{r-1} \sum_{j=i+1}^{r} \left(\sum_{k=i}^{j-1} a_k \right) [x_i, x_j] \\ = a_1 y_1 + \cdots + a_r y_r &+ \frac{1}{2} \sum_{i=1}^{r-1} \sum_{j=i+1}^{r} \left(\sum_{k=i}^{j-1} a_k \right) \left(\sum_{l=j}^{r} a_l \right) [x_i, x_j], \end{aligned}$$

and so the result is true for $n = r$ as required. □

With this result and the following observation we will be able to construct our required U.B.

Lemma 1·18. *Let P be a regular p-group of exponent p and with a C.B. $B = (y_1, \ldots, y_k)$. Then $y_i \in Z(P)$ for some i, $1 \leq i \leq k$.*

Proof. Since B is a canonical basis there exists a normal subgroup Q of P with $|Q : \mathbf{U}_1(P)| = p$ and containing exactly one element of B. Therefore since P has exponent p it follows that Q must be a central subgroup and so B contains a central element of P. □

Proposition 1·19. *Let P be a p-group of exponent p and nilpotency class 2. Then P possesses a U.B. which is not a C.B.*

Proof. Let $|P| = p^n$, $|Z(P)| = p^{n-r}$ (where $n \geq 3$ and $1 \leq r \lneqq n$ since P is non-Abelian) and, regarding $\mathcal{L}_p(P)$ as an F_p-Lie algebra (since P has exponent p), choose an F_p-basis $x_1, \ldots, x_r, x_{r+1}, \ldots, x_n$ for $\mathcal{L}_p(P)$ subject to the condition that $x_{r+1}, \ldots, x_n$ span the centre of $\mathcal{L}(P)$. Now define a sequence $B = (y_1, \ldots, y_n)$ of elements of $\mathcal{L}_p(P)$ by

$$y_i = \sum_{j=1}^{i} x_j \quad \text{for } i = 1, \ldots, n.$$

Observe that B contains no central elements of $\mathcal{L}_p(P)$ and so since $Z(P) = Z\big(\mathcal{L}(P)\big)$ the theorem will be proved if we can show that B is a U.B. of P (since lemma 1·18 shows that a C.B. of P must contain a central element of P).

So let $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{Z}$ and suppose that

$$y_1^{a_1} \cdots y_n^{a_n} = y_1^{b_1} \cdots y_n^{b_n}, \tag{1·11}$$

and observe that we must show that $a_i \equiv b_i \pmod{p}$ for each $i = 1, \ldots, n$. To do this we first apply lemma 1·17 to both sides of (1·11) which gives us

$$\begin{aligned} a_1 y_1 + \cdots + a_n y_n + \frac{1}{2} \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} \Big(\sum_{k=i}^{j-1} a_k \Big) \Big(\sum_{l=j}^{n} a_l \Big) [x_i, x_j] \\ = b_1 y_1 + \cdots + b_n y_n + \frac{1}{2} \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} \Big(\sum_{k=i}^{j-1} b_k \Big) \Big(\sum_{l=j}^{n} b_l \Big) [x_i, x_j], \end{aligned}$$

and since $x_{r+1}, \ldots, x_n$ are central elements of $\mathcal{L}_p(P)$ we obtain

$$a_1y_1 + \cdots + a_ny_n + \frac{1}{2}\sum_{i=1}^{r-1}\sum_{j=i+1}^{r}\Big(\sum_{k=i}^{j-1}a_k\Big)\Big(\sum_{l=j}^{n}a_l\Big)[x_i,x_j]$$
$$= b_1y_1 + \cdots + b_ny_n + \frac{1}{2}\sum_{i=1}^{r-1}\sum_{j=i+1}^{r}\Big(\sum_{k=i}^{j-1}b_k\Big)\Big(\sum_{l=j}^{n}b_l\Big)[x_i,x_j]$$

Equating elements of the centre and the coefficients of $x_1, \ldots, x_r$ in this equation we obtain the following equation and r congruences

$$\sum_{i=r+1}^{n}\Big(\sum_{j=i}^{n}a_j\Big)x_i + \frac{1}{2}\sum_{i=1}^{r-1}\sum_{j=i+1}^{r}\Big(\sum_{k=i}^{j-1}a_k\Big)\Big(\sum_{l=j}^{n}a_l\Big)[x_i,x_j]$$
$$= \sum_{i=r+1}^{n}\Big(\sum_{j=i}^{n}b_j\Big)x_i + \frac{1}{2}\sum_{i=1}^{r-1}\sum_{j=i+1}^{r}\Big(\sum_{k=i}^{j-1}b_k\Big)\Big(\sum_{l=j}^{n}b_l\Big)[x_i,x_j] \tag{1·12}$$

$$\sum_{i=k}^{n}a_i \equiv \sum_{i=k}^{n}b_i \pmod{p} \quad \text{for each } k = 1, \ldots, r \tag{1·13}$$

Now the r congruences in (1·13) show us that $a_i \equiv b_i \pmod{p}$ for $i = 1, \ldots, r-1$, and so for $1 \leq i \lneqq j \leq r$ we get

$$\sum_{k=i}^{j-1}a_k \equiv \sum_{k=i}^{j-1}b_k \pmod{p}. \tag{1·14}$$

Using (1·14) together with the congruences in (1·13) we obtain the equation

$$\frac{1}{2}\sum_{i=1}^{r-1}\sum_{j=i+1}^{r}\Big(\sum_{k=i}^{j-1}a_k\Big)\Big(\sum_{l=j}^{n}a_l\Big)[x_i,x_j] = \frac{1}{2}\sum_{i=1}^{r-1}\sum_{j=i+1}^{r}\Big(\sum_{k=i}^{j-1}b_k\Big)\Big(\sum_{l=j}^{n}b_l\Big)[x_i,x_j],$$

and therefore (1·12) becomes

$$\sum_{i=r+1}^{n}\Big(\sum_{j=i}^{n}a_j\Big)x_i = \sum_{i=r+1}^{n}\Big(\sum_{j=i}^{n}b_j\Big)x_i. \tag{1·15}$$

Equating coefficients of $x_{r+1}, \ldots, x_n$ in (1·15) gives us the $n-r$ congruences

$$\sum_{j=i}^{n}a_j \equiv \sum_{j=i}^{n}b_j \pmod{p} \quad \text{for each } i = r+1, \ldots, n,$$

and we therefore have $a_i \equiv b_i \pmod{p}$ for each $i = 1, \ldots, n$, as required. □

We now consider briefly the connection between canonical and uniqueness bases of a p-group P in Γ_p, and bases of the corresponding Lie ring $\mathcal{L}_p(P)$. If we let B be a canonical basis of P then from the definition given in section 1·2 it follows that there exists a chain $P = Q_0 \triangleright Q_1 \triangleright \cdots \triangleright Q_{\omega_1} = U_1(P)$ of normal subgroups of P where for each $i = 0, \ldots, \omega_1 - 1$, $Q_i \setminus Q_{i+1}$ contains exactly one element of B, and the product of the orders of the elements of B equals $|P|$. Now this chain is also a chain of ideals of $\mathcal{L}_p(P)$ and hence is a chain of subgroups of the Abelian (and hence regular) p-group $(\mathcal{L}_p(P), +)$. So using the fact that this chain terminates at $U_1(\mathcal{L}_p(P))$ and the fact that the order of an element of B is the same whether it is regarded as an element of P or $(\mathcal{L}_p(P), +)$, we see that B is a canonical basis of $(\mathcal{L}_p(P), +)$. But for Abelian p-groups the notion of canonical basis coincides with the notion of uniqueness basis and so B is a uniqueness basis of $(\mathcal{L}_p(P), +)$ i.e. a basis of the Lie ring $\mathcal{L}_p(P)$. Hence a canonical basis of P is a basis of $\mathcal{L}_p(P)$, and proposition 1·19 showed that the converse is not in general true.

The remaining question to consider is the connection between uniqueness bases of P and bases of $\mathcal{L}_p(P)$. The following example shows that for any p-group P of exponent p and nilpotency class 2, there is a basis of $\mathcal{L}_p(P)$ which is not a uniqueness basis of P.

Example. Let P be a p-group of exponent p and nilpotency class 2. Choose an $\mathbb{F}_p$-basis $(x_1, \ldots, x_n)$ of $\mathcal{L}_p(P)$ where we have $n \geq 3$ and can assume that $[x_1, x_2] \neq 0$ since P is non-Abelian. If we express $[x_1, x_2]$ in the form

$$[x_1, x_2] = \sum_{i=1}^{n} \alpha_i x_i, \quad \text{where } \alpha_i \in \mathbb{Z} \text{ for each } i = 1, \ldots, n,$$

then nilpotency of $\mathcal{L}_p(P)$ implies that α_j must be coprime to p for some j with $3 \leq j \leq n$. It therefore follows that we can replace the basis element x_j with the element $x_1 + x_2 + \frac{1}{2}[x_1, x_2]$ to get a new basis where the Campbell-Hausdorff product (i.e. the group product in P) of x_1 and x_2 is the element x_j which shows that this basis of $\mathcal{L}_p(P)$ cannot be a U.B. of P.

The question of whether a uniqueness basis of P is necessarily a basis of $\mathcal{L}_p(P)$ seems to be more difficult than the questions considered so far. In the remainder of this chapter we show how to reduce this question to groups of exponent p and use this to show that

if P is a p-group in Γ_p with $\omega_1(P) \leq 3$ then any uniqueness basis of P is automatically a basis for $\mathcal{L}_p(P)$. Observe that this shows that unlike the examples given in proposition 1·19 and the above example, no counterexample exists in a group of order 27 (the smallest possible order of a non-Abelian regular p-group). To show how to reduce the above question to groups of exponent p we first need an easy lemma on Abelian p-groups.

Lemma 1·20. *Let A be an Abelian p-group of type $(\mu_1, \ldots, \mu_{\omega_1})$ and suppose that $X = (x_1, \ldots, x_{\omega_1})$ is a sequence of elements of A which is not a basis and for each $i = 1, \ldots, \omega_1$, the order of x_i is p^{μ_i}. Then the natural image $\overline{X}$ of X in the elementary Abelian p-group $A/\mathfrak{U}_1(A)$ is not a basis.*

Proof. Observe that A must be non-cyclic (i.e. $\omega_1 \geq 2$) and we can assume that $x_i \notin \mathfrak{U}_1(A)$ for each $i = 1, \ldots, \omega_1$ (the result is clear if not). Let r be the maximum integer such that X possesses a subsequence $(x_{i_1}, \ldots, x_{i_r})$ which can be extended to a basis $Y = (x_{i_1}, \ldots, x_{i_r}, y_1, \ldots, y_{\omega_1 - r})$ of A (so $1 \leq r \leq \omega_1 - 1$), and suppose that $(\gamma_1, \ldots, \gamma_{\omega_1 - r})$ are the type invariants corresponding to $(y_1, \ldots, y_{\omega_1 - r})$ where we assume that $\gamma_1 \leq \gamma_2 \leq \cdots \leq \gamma_r$. By the condition on the orders of the elements of X we can choose some element x_j of X which is not in Y and has the same order as y_1. Expressing x_j as a $\mathbb{Z}-$linear combination of the basis Y, viz.

$$x_j = \sum_{l=1}^{r} a_l x_{i_l} + b_1 y_1 + \cdots + b_{\omega_1 - r} y_{\omega_1 - r}\,, \tag{1·16}$$

it follows that since $x_j \notin \mathfrak{U}_1(A)$ either some a_l is coprime to p or some b_m is coprime to p. If $(b_m, p) = 1$ for some m, $1 \leq m \leq \omega_1 - r$, then we must have $\gamma_m = \gamma_1$, but this implies that $\langle x_j \rangle \cap \langle x_{i_1}, \ldots, x_{i_r}, y_1, \ldots, y_{m-1}, y_{m+1}, \ldots, y_{\omega_1 - r} \rangle = \{0\}$ which would contradict the choice of r. Hence $p \mid b_1, \ldots, b_{\omega_1 - r}$ and $(a_l, p) = 1$ for some l, $1 \leq l \leq r$, and then the image of (1·16) in $A/\mathfrak{U}_1(A)$ gives the required non-trivial relation. □

It is now a straightforward matter to reduce the question of whether a uniqueness basis is a Lie ring basis to the exponent p situation. We suppose that P is a p-group in Γ_p which possesses a uniqueness basis $B = (x_1, \ldots, x_{\omega_1})$ which is not a basis of $\mathcal{L}_p(P)$. If we denote by $\overline{B} = (\overline{x}_1, \ldots, \overline{x}_{\omega_1})$ the image of B in $\overline{P} = P/\mathfrak{U}_1(P)$, then it follows from the fact

that $|P : \mathfrak{U}_1(P)| = p^{\omega_1}$ that $\overline{B}$ is a uniqueness basis of $\overline{P}$. Now by lemma 1·6 we know that

$$\mathcal{L}_p(\overline{P}) = \mathcal{L}_p(P)/\mathfrak{U}_1(\mathcal{L}_p(P))$$

and so by lemma 1·20 we see that $\overline{B}$ is not a Lie ring basis of $\mathcal{L}_p(\overline{P})$, as required. Using this reduction we can now show the following result.

Proposition 1·21. *Let P be in Γ_p with $\omega_1(P) \leq 3$. Then any uniqueness basis of P is a basis of $\mathcal{L}_p(P)$.*

Proof. By the above discussion it suffices show the result in the case that P has exponent p, and so we may assume that $|P| \leq p^3$. If P is Abelian then the result clearly holds so the only case to consider is when P is the unique non-Abelian p-group of order p^3 and exponent p. So suppose (for a contradiction) that P possesses a uniqueness basis (u, v, w) which does not form an F_p−basis of $\mathcal{L}_p(P)$ (and therefore the subspace of $\mathcal{L}_p(P)$ spanned by $\{u, v, w\}$ has dimension 2). Now since the subgroups generated by any two distinct elements of a uniqueness basis must have trivial intersection, it follows that we can express w as $w = \alpha u + \beta v$ where $\alpha, \beta \in \mathbb{Z}$ with $\alpha, \beta \not\equiv 0 \pmod{p}$. Also, since we are assuming that (u, v, w) is a U.B. we must have $[u, v] \neq 0$ (otherwise $w = u^\alpha v^\beta$), which then implies (by nilpotency) that $[u, v] \notin \langle u, v \rangle$. Therefore, defining $z = [u, v]$, the sequence (u, v, z) is an F_p−basis of $\mathcal{L}_p(P)$.

Now let $a, b, c \in \mathbb{Z}$. Then

$$\begin{aligned} u^a v^b w^c &= au + bv + \frac{ab}{2} z + cw + \frac{1}{2}(ac[u, w] + bc[v, w]) \\ &= (a + \alpha c)u + (b + \beta c)v + \frac{1}{2}(ab + \beta ac - \alpha bc)z. \end{aligned}$$

Now since (u, v, w) is a U.B. each element of $\mathcal{L}_p(P)$ and hence, in particular, each element of $\langle z \rangle$ must be representable in this form. So, for an arbitrary element $\gamma z \in \langle z \rangle$ (with γ an integer), the following congruences must have a unique solution modulo p for a, b and c:

$$\begin{aligned} a + \alpha c &\equiv 0 \pmod{p} \\ b + \beta c &\equiv 0 \pmod{p} \\ ab + \beta ac - \alpha bc &\equiv 2\gamma \pmod{p}. \end{aligned}$$

These equations then imply that

$$c^2\alpha\beta \equiv 2\gamma \pmod{p}$$

is always soluble for c. But since p is odd this implies that $2\gamma(\alpha\beta)^{-1}$ is a quadratic residue modulo p for all integers $\gamma \not\equiv 0 \pmod{p}$ which gives the desired contradiction. □

Chapter 2. The Class and Coexponent of a Finite p-Group

Section 2·1. Introduction and Statement of Main Theorems.

For a prime p and a finite p-group P, we define the **coexponent** of P to be the least integer $f(P)$ such that P possesses a cyclic subgroup of index $p^{f(P)}$. So for instance, a finite p-group P has coexponent 0 precisely if it is cyclic, and in this chapter we are concerned with deriving a bound for the nilpotency class of a finite p-group in terms of its coexponent. We will have to exclude the prime 2 from the outset since if n is a natural number greater than 2 then the group $C_{2^{n-1}} \rtimes C_2$ where the cyclic group acts by inversion, is a group of order 2^n which has coexponent 1 and nilpotency class $n-1$.

The research for this chapter is joint with Dr. T. Wilde and has appeared in preprint form as [25]. In the remainder of this section we present the statements of our two main theorems leaving the proofs to section 2.3. Since we will be using certain results about p-groups of maximal class, we summarise these results in section 2.2. for convenience.

Our main theorem generalises the well-known fact that if p is an odd prime then any p-group P with $f(P) = 1$ (i.e. non-cyclic and containing a cyclic maximal subgroup) has nilpotency class at most 2 (see e.g. [28] 4.1.(a)).

Theorem 2·1. *Let p be an odd prime and P a finite p-group of coexponent $f(P) \geq 1$. Then $cl(P) \leq 2f(P)$.*

The bound in theorem 2·1 is clearly attained by taking P to be a non-Abelian p-group containing a cyclic maximal subgroup (for $p > 2$). However, an examination of the proof we give in section 2.3 together with certain results on regular p-groups and p-groups of maximal class will enable us to show that this bound is attained only if $f(P) = 1$ or $p = 3$. We then have

Theorem 2·2. *Let p be a prime greater than 3 and P a finite p-group of coexponent $f(P) \geq 2$. Then $cl(P) \leq 2f(P) - 1$.*

In this chapter, for an integer $i \geq 2$, the $i^{\text{th}}-$term of the lower central series of a group G will be denoted by G_i, and if H, K are subgroups of G then $[H, K]$ denotes the commutator group of H and K.

Section 2·2. Background Results on p-Groups of Maximal Class.

In this section we briefly state the results we shall use concerning p-groups of maximal class. The results collated here are originally due to Blackburn [2], although the citations given here indicate where the proofs are to be found in Chapter III §14 of Huppert's book [9].

If P is a p-group of order p^n with $n \geq 2$ then it is easy to see that $\gamma_n(P) = 1$ and so P has nilpotency class at most $n-1$. P is said to be a **p-group of maximal class** if it has nilpotency class exactly $n-1$. For $n \geq 3$ the normal subgroup lattice of such a group consists of the terms of the lower central series together with its $p+1$ maximal subgroups. Of principal importance is the maximal subgroup P_1 given in the following definition.

Definition 1. *Let P be a p-group of maximal class with $|P| = p^n$ and $n \geq 4$. For $i \geq 2$ we define P_i to be $\gamma_i(P)$ (the i-th term of the lower central series of P), and then define P_1 by*

$$P_1 = C_P\left(P_2/P_4\right).$$

Definition 2. *Let P be a p-group of maximal class with $|P| = p^n$ and $n \geq 5$. P is called* **exceptional** *if there exists some i, $1 \leq i \leq n-2$ such that $P_1 \neq C_P(P_i/P_{i+2})$, i.e. if $[P_i, P_1] = P_{i+1}$.*

Theorem 2·3. ([9] 14.6.(b)) *Let P be a p-group of maximal class with $|P| = p^n$ and $n \geq 5$. If P is exceptional then $p > 3$ and, moreover, $6 \leq n \leq p+1$ and n is even.*

Thus if n is odd (the situation we will be considering) then P is not exceptional and the following result can be invoked with x taken to be any element of $P \setminus P_1$ (a non-empty set).

Theorem 2·4. ([9] 14.13.(b)) *Let P be a p-group of maximal class with $|P| = p^n$ $(n \geq 4)$ and suppose that x is an element of P with the property that $x \notin C_P(P_i/P_{i+2})$ for each $i = 2, \ldots, n-2$. Then, $O(x) \leq p^2$.*

This theorem will be used to show that elements of order greater than p^2 must lie in P_1 (since the groups we will consider are not exceptional by the above remark).

Theorem 2·5. ([9] 14.14.) *Let P be a p-group of maximal class with $|P| = p^n$ and $5 \leq n \leq p+1$. Then P/P_{n-1} and P_2 have exponent p.*

Thus if $n \geq 5$ and P has exponent greater than p^2 we must have $p < n-1$ and then we are able to apply the following theorem.

Theorem 2·6. ([9] 14.16.) *Let P be a p-group of maximal class with $|P| = p^n$ and $n > p+1$. Then $\mathfrak{U}_1(P_i) = P_{i+p-1}$ for all i, $1 \leq i \leq n-p+1$. Also, P_1 is a regular p-group with $\Omega_1(P_1) = P_{n-p+1}$.*

Section 2·3. Proofs.

Let p be an odd prime and P a finite p-group of order p^n and coexponent $f = f(P) \geq 1$. It may be assumed that $n > 2f$ since both 2·1 and 2·2 are trivially true otherwise. We begin by examining the core of a largest cyclic subgroup contained in P, so let $a \in P$ have order p^{n-f} and define subgroups Q and N of P to be $\langle a \rangle$ and $\mathrm{Core}_P(\langle a \rangle)$ respectively.

Lemma 2·7. *Defining integers r and s by $p^r = \min\{|P : QQ^b| : b \in P\}$, and $p^{r-s} = |P : C_P(N)|$ we have*

i) $1 \leq r \leq f$ *and* $|P : N| = p^{2f-r}$.

ii) $s \geq 0$, *and* $[[\ldots,[N,\underbrace{P],\ldots],P}_{u \text{ times}}] \leq \mathfrak{U}_{(n-2f)u}(N)$, *for any integer* $u \geq 1$.

Proof.

i) It is easy to see that no group is the product of two proper conjugate cyclic subgroups and so it follows that $1 \leq r \leq f$. To see that $|P : N| = p^{2f-r}$ observe that for any element b of P we have

$$|Q : Q \cap Q^b| = |QQ^b : Q|.$$

Now since Q is cyclic there exists some element c of P with $\mathrm{Core}_P(Q) = Q \cap Q^c$ and then for any other $b \in P$ we have

$$Q \geq Q \cap Q^b \geq Q \cap Q^c,$$

whence $|QQ^c : Q| \geq |QQ^b : Q|$. Therefore $|Q : N| = \max\{|QQ^b : Q| : b \in P\} = p^{f-r}$ and so $|P : N| = p^{2f-r}$.

ii) Let c be defined as in i). Then since N is centralised by both Q and Q^c it follows that $QQ^c \leq C_P(N)$ and so $s \geq 0$. Now let k be an integer satisfying $1 \leq k \leq n - 2f + r$ (observe by (i) that $|N| = p^{n-2f+r}$ and $n - 2f + r \geq 2$). Because N is a cyclic group of prime-power order, any automorphism of $N/\mathfrak{U}_k(N)$ lifts to an automorphism of N and so we have a composite of maps

$$P \xrightarrow{\phi} \mathrm{Aut}(N) \xrightarrow{\gamma} \mathrm{Aut}\left(N/\mathfrak{U}_k(N)\right)$$

where P acts by conjugation on N and γ is onto. It follows that

$$|\mathrm{Im}(\phi)| = |P : C_P(N)| \quad \text{and} \quad |\mathrm{Ker}(\gamma)| = \frac{p^{n-2f+r-1}(p-1)}{p^{k-1}(p-1)}.$$

Since p is odd we have that $\mathrm{Aut}(N)$ is cyclic, and therefore $\mathrm{Im}(\phi) \subseteq \mathrm{Ker}(\gamma)$ if and only if $n - 2f + r - k \geq r - s$, i.e. if and only if $k \leq n - 2f + s$. So taking $k = n - 2f$ we see that $[N, P] \subseteq \mathfrak{U}_k(N)$ and then the desired result follows by using induction on u and the fact that for any $l \geq 0$, $\left[\mathfrak{U}_l(N), P\right] \subseteq \mathfrak{U}_l([N, P])$. □

Proof of Theorem 2·1.

Using the same notation as above we may assume that $|P : N| \geq p^2$ since otherwise P contains a cyclic maximal subgroup and this is the well-known case mentioned in the introduction. Hence if we set $k = \mathrm{cl}(P/N)$ then $1 \leq k \leq 2f - r - 1$ by part i) of lemma

2·7, and so using part ii) of lemma 2·7 we obtain $P_{k+u+1} \subseteq \mathfrak{U}_{(n-2f)u}(N)$ for any integer $u \geq 1$. So since $|N| = p^{n-2f+r}$ it follows that if u is an integer greater than or equal to 1 and $(n-2f)u \geq n-2f+r$ then $P_{k+u+1} = 1$. Hence,

$$\mathrm{cl}(P) \leq \mathrm{cl}\left(P/N\right) + \left\lceil \frac{n-2f+r}{n-2f} \right\rceil + 1 - 1 = \mathrm{cl}\left(P/N\right) + \left\lceil \frac{r}{n-2f} \right\rceil + 1,$$

where the symbol $\lceil x \rceil$ denotes the least integer greater than or equal to x ($\in \mathbb{R}$). Therefore, substituting for $\mathrm{cl}(P/N)$ we have

$$\mathrm{cl}(P) \leq 2f - r - 1 + \left\lceil \frac{r}{n-2f} \right\rceil + 1 = 2f + \left\lceil r\left(\frac{1}{n-2f} - 1\right) \right\rceil \qquad (2\cdot1)$$

which, since $n - 2f \geq 1$ by assumption, is less than or equal to $2f$ as required. □

To prove Theorem 2·2 we determine the situations under which the right-hand side of equation (2·1) actually attains the value $2f$, and show that unless $f(P) = 1$ or $p = 3$ the bound on the class can be improved to $2f(P) - 1$. As mentioned in the introduction, there exist groups with $f(P) = 1$ and nilpotency class 2, therefore we will assume $f(P) > 1$ so that equation (2·1) applies to any group we consider. We also continue to use the notation already developed above. Observe that there are two possible situations under which the right-hand side of equation (2·1) can have the value $2f(P)$:

i) $n - 2f = 1$, i.e. $|P| = p^{2f+1}$.

ii) $n - 2f > 1$ and $r = 1$.

The following lemma shows that in case i) the nilpotency class is never equal to $2f$.

Lemma 2·8. *Let p be an odd prime and P a p-group of coexponent $f = f(P) > 1$ with $|P| = p^n$ where $n = 2f + 1$. Then $\mathrm{cl}(P) \leq 2f - 1$, i.e. P does not have maximal class.*

Proof. Suppose that P does have maximal class $2f$ (for a contradiction) and define Q, N and r as above. Since $r \geq 1$ it follows that $|N| \geq p^2$ and because P has maximal class with $|P : N| \geq p^2$ we know that $N = P_{2f-r}$. Now, $|Q| = p^{f+1} > p^2$ and $n = 2f + 1 \geq 5$, therefore by theorem 2·5 we must have $p < n - 1$, in which case we can apply theorem 2·6 to deduce that P_{n-p+1} has exponent p. Therefore $N \not\subseteq P_{n-p+1}$, i.e. $2 \leq 2f - r < n - p + 1$. We can now apply theorem 2·6 again with $i = 2f - r$ to obtain that

$$\mathfrak{U}_1(N) = P_{2f-r+p-1} \subsetneq P_{2f-r+1} \qquad (2\cdot2)$$

Since P has maximal class each term of the lower central series has index p in the one above (apart from P_2) and so we must have $|N : P_{2f-r+1}| = p$. But since N is cyclic it has a unique subgroup of index p and so $\mho_1(N) = P_{2f-r+1}$ which contradicts equation (2·2). □

So we may assume that $n - 2f > 1$ and focus on case ii) above which is trickier to resolve. In this situation the group P/N has order $2f(P) - 1$ and contains a cyclic subgroup Q/N which has index $p^{f(P)}$ and trivial core. The next lemma shows that if P/N has maximal class and $f(P) \geq 3$ then we must have $p = 3$. Thus, if we are in case ii) above with $f(P) \geq 3$ and $p > 3$ then 1 can be subtracted from the right-hand side of equation (2·1) when substituting for $\mathrm{cl}(P/N)$ thereby bounding the class of P by $2f(P) - 1$.

Lemma 2·9. *Let p be an odd prime and G a p-group with $|G| = p^{2k-1}$ where $k \geq 3$. Suppose further that G contains a cyclic subgroup H of index p^k which has trivial core. Then G does not have maximal class except, possibly, when $p = 3$.*

Proof. We consider the two cases $k = 3$ and $k \geq 4$ separately.

a) $k = 3$.

We suppose that $p \geq 5$ and show that $cl(G) \leq 2k - 3 = 3$, so let G be a group of order p^5 which contains a cyclic subgroup H of index p^3 with $\mathrm{Core}_G(H) = 1$. Suppose (for a contradiction) that G has maximal class 4. Then since the hypotheses of theorem 2·5 are satisfied we have that G/G_4 has exponent p, and because $Z(G) = G_4$ we know that $H \cap G_4 \subseteq \mathrm{Core}_G(H) = 1$. Therefore HG_4/G_4 has order p^2 and is a cyclic subgroup of G/G_4 which contradicts the fact that G/G_4 has exponent p. Hence $cl(G) \leq 3$ as required.

b) $k \geq 4$.

We suppose that G has maximal class $2k-2$ and show that $p = 3$. Since n $(= 2k-1)$ is odd we know that G is not exceptional (by theorem 2·3) and so for any i with $2 \leq i \leq n-2$, we have $G_1 = C_G(G_i/G_{i+2})$. Therefore by an application of theorem 2·4 it follows that all elements of G which have order greater than p^2 must lie in G_1. In particular, H and all its conjugates are contained in G_1. So choosing $x \in G$ with $H \cap H^x = 1$ (recall that H has trivial core) we have that $|H||H^x| = p^{2k-2}$. Therefore since G_1 is a (proper) maximal

subgroup it follows that $G_1 = HH^x$. Now since the exponent of G is greater than p^2 we must have $3 \leq p < n-1$ (by theorem 2·5), and then theorem 2·6 gives us that G_1 is a regular p-group . From the above factorisation of G_1 we can see that $|G_1 : \mho_1(G_1)| \leq p^2$ and $|\Omega_1(G_1)| \geq p^2$, and so by part iv) of theorem 1·7 these two inequalities are equalities which then implies that $\Omega_1(G_1) = G_{n-2}$ (since $\Omega_1(G_1)$ is a normal subgroup of G and G has maximal class). But we also know (by theorem 2·6) that $\Omega_1(G_1) = G_{n-p+1}$ and so $n-p+1 = n-2$, i.e. $p = 3$ as required. □

We have now shown that Theorem 2·2 holds for all coexponents greater than 2. Since Lemma 2·9 is not true for $k = 2$ we deal with the coexponent 2 case directly in the following lemma.

Lemma 2·10. *Let p be a prime greater than 3 and P a p-group of coexponent $f(P) = 2$. Then* $\mathrm{cl}(P) \leq 2f(P) - 1$.

Proof. By Theorem 2·1 the bound $2f(P)$ holds and so since $p > 2f(P)$ it follows that $\mathrm{cl}(P) < p$ which implies that P is regular by theorem 1·9, hence if we let $|P| = p^n$ then P is of *type* $(n-2,2)$ or *type* $(n-2,1,1)$. If P is of *type* $(n-2,2)$ then $|P : \mho_1(P)| = p^2$ and so $[P,P] \subseteq \mho_1(P)$. Then by applying theorem 1·15 with $\alpha = \beta = 1$ we obtain that $P_3 \subseteq \mho_2(P)$. By taking a U.B. of P it is straightforward to see that $\mho_2(P) \subseteq Z(P)$ and therefore $\mathrm{cl}(P) \leq 3 = 2f(P) - 1$. If P is of *type* $(n-2,1,1)$ then the p^{th}-power of a basis element corresponding to the invariant $n-2$ is central by corollary 1·8, and so $|P : Z(P)| \leq p^3$, from which the required bound follows. □

We have now completed the proof of theorem 2·2.

Chapter 3. The Class and Coexponent of a Regular p-Group

Section 3·1. Introduction.

In this chapter we show how the bounds obtained in chapter 2 can be improved upon if we restrict attention to regular p-groups. The first improvement we make is to consider the bound given in theorem 2·2 in the context of regular p-groups and we show that in this situation one can be subtracted from the bound provided that the coexponent is greater than 2. To achieve this we argue directly by using the type invariants and corresponding bases associated with a regular p-group (see section 1·2).

For the second improved bound, we first observe that a consequence of Theorem 2·1 is that for a fixed coexponent f we automatically have regularity for any p-group P with $f(P) = f$ provided that $p > 2f$, and so it follows that the first improved bound holds for all but finitely many primes once the coexponent f is fixed. It is therefore natural to ask exactly what bound is possible if we allow ourselves to restrict attention to a cofinite set of primes for each coexponent. The second improvement we obtain shows that by excluding finitely many primes p for each coexponent f, any finite p-group of coexponent f (where p is not one of the excluded primes) has nilpotency class at most $f + 1$. Moreover, we give a constructive example to show that for any f this bound is attained for arbitrarily large primes p, thereby answering the question completely.

The argument we use is less direct than the first improvement and is obtained by first considering the corresponding problem for Lie rings and then using the functorial correspondence of section 1·1·3 to reinterpret the solution in terms of finite p-groups (this approach works since the excluded primes ensure that the nilpotency class is less than p and so the Lie ring correspondence is applicable).

Notational remarks. In this chapter we will continue using the notation of chapter 2 by denoting the i^{th} term of the lower central series of a group or Lie ring K by K_i, where $i \geq 2$. Also, if Y is a subset of a Lie ring L then $\langle Y \rangle$ will denote the subgroup of $(L, +)$

generated by Y (this is contained in the subring generated by Y but equality need not necessarily hold).

Section 3·2. An Improved Bound.

In this section we freely use the notation concerning regular p-groups which was introduced in section 1·2. So let p be an arbitrary prime and P a regular p-group of *type* $(\mu_1, \ldots, \mu_{\omega_1})$ where we assume that ω_1 is greater than 1 (i.e. P is non-cyclic), so that P has coexponent $f(P) = \Sigma_{i=2}^{\omega_1} \mu_i$. Now letting $(g_1, \ldots, g_{\omega_1})$ be a *U.B.* of P corresponding to the type invariants (i.e. for each $i = 1, \ldots, \omega_1$, g_i has order p^{μ_i} – see theorem 1·14), we have the following lemma.

Lemma 3·1.

i) $\mathrm{cl}(P) \leq f(P) + \mu_2$.

ii) *If* $\omega_1 = 2$ *then* $\mathrm{cl}(P) \leq \mu_2 + 1$.

iii) *If* $\omega_1 > 2$ *and* $\mu_2 > \mu_3$ *then* $\mathrm{cl}(P) \leq f(P) + \mu_2 - 1$.

Proof.

i) For $2 \leq i \leq \omega_1$ we have $[g_1, g_i^{p^{\mu_2}}] = 1$ and so by corollary 1·8 it follows that $[g_1^{p^{\mu_2}}, g_i] = 1$. Hence $g_1^{p^{\mu_2}}$ centralises all elements of the U.B. and so $g_1^{p^{\mu_2}} \in Z(P)$. Now $|P : \langle g_1^{p^{\mu_2}} \rangle| = p^{f(P)+\mu_2}$ so that $P_{f(P)+\mu_2} \subseteq Z(P)$ which implies that $\mathrm{cl}(P) \leq f(P) + \mu_2$.

ii) If $\omega_1 = 2$ then by part iv) of theorem 1·7 we know that $|P : \mathfrak{U}_1(P)| = p^2$ and so $P_2 \subseteq \mathfrak{U}_1(P)$, from which it follows (by theorem 1·15) that $P_{\mu_2+1} \subseteq \mathfrak{U}_{\mu_2}(P)$. Also, from part ii) of theorem 1·14 we know that $\mathfrak{U}_{\mu_2}(P) = \langle g_1^{p^{\mu_2}} \rangle$ and since $g_1^{p^{\mu_2}} \in Z(P)$ (as in (i)) we have $\mathrm{cl}(P) \leq \mu_2 + 1$.

iii) Let $\overline{P}$ denote the quotient group $P/\langle g_1^{p^{\mu_2}} \rangle$ and for $1 \leq i \leq \omega_1$, set $\overline{g}_i = g_i \langle g_1^{p^{\mu_2}} \rangle \in \overline{P}$. Then $\overline{P}$ is regular (a quotient of a regular p-group is regular — immediate from the definition) and $(\overline{g}_1, \ldots, \overline{g}_{\omega_1})$ is a U.B. of $\overline{P}$ so that $\overline{P}$ is of *type* $(\mu_2(P), \mu_2(P), \mu_3(P), \ldots, \mu_{\omega_1}(P))$. Hence by part ii) of theorem 1·14 and the fact that $\mu_2 > \mu_i$ for each $i = 3, \ldots, \omega_1$, we see that

$$\Omega_{\mu_2-1}(\overline{P}) = \langle \overline{g}_1{}^p \rangle \langle \overline{g}_2{}^p \rangle \langle \overline{g}_3 \rangle \cdots \langle \overline{g}_{\omega_1} \rangle.$$

Therefore, $|\overline{P} : \Omega_{\mu_2-1}(\overline{P})| = p^2$ from which it follows that $[\overline{g}_1, \overline{g}_2] \in \Omega_{\mu_2-1}(\overline{P})$ and so $\overline{g}_1{}^{p^{\mu_2-1}}, \overline{g}_2{}^{p^{\mu_2-1}} \in Z(\overline{P})$. Hence $|\overline{P} : Z(\overline{P})| \leq p^{\mu_2+f(P)-2}$ and so we see that $P_{f(P)+\mu_2-1} \subseteq \langle g_1^{p^{\mu_2}} \rangle \subseteq Z(P)$, which implies that $\mathrm{cl}(P) \leq f(P) + \mu_2 - 1$. □

Using this lemma we can obtain the the first improved bound as mentioned in the introduction.

Theorem 3·2. *Let P be a regular p-group with $f(P) > 2$. Then* $\mathrm{cl}(P) \leq 2(f(P) - 1)$.

Proof. Since P is non-cyclic we know that $\omega_1(P) \geq 2$ so consider the cases $\omega_1(P) = 2$ and $\omega_1(P) > 2$ separately. If $\omega_1(P) = 2$ then by part ii) of lemma 3·1 we know that $\mathrm{cl}(P) \leq \mu_2(P) + 1$ and since $f(P) = \mu_2(P)$ (in this case) and $f(P) - 2 \geq 1$ we therefore have $\mathrm{cl}(P) \leq 2(f(P) - 1)$. Now consider the case $\omega_1(P) > 2$. By part i) of lemma 3·1 we know that $cl(P) \leq f(P) + \mu_2(P)$ and this is less than or equal to $2(f(P) - 1)$ unless $\mu_2(P) > f(P) - 2$, i.e. $\mu_2(P) = f(P) - 1$. But in this situation $\mu_3(P) = 1$ which is less than $\mu_2(P)$ (since $f(P) \geq 3$), and so by part iii) of lemma 3·1 we have $\mathrm{cl}(P) \leq f(P) + \mu_2(P) - 1 = 2(f(P) - 1)$, as required. □

We conclude this section with a constructive example which indicates the bound we seek for the second improvement as mentioned in the introduction (see note (ii) following this example).

Example. Let $f \geq 1$, $n \geq f+2$ and p a prime greater than or equal to $f+1$. Let A be the elementary Abelian p-group $\underbrace{C_p \times \cdots \times C_p}_{f+1 \text{ times}}$ and, regarding A as an $(f+1)-$dimensional vector space over F_p (the field with p elements), consider an automorphism α of A which is represented by the matrix

$$\begin{pmatrix} 1 & 1 & & \\ & 1 & \ddots & \\ & & \ddots & 1 \\ & & & 1 \end{pmatrix} \in \mathrm{GL}_{f+1}(\mathsf{F}_p)$$

relative to some basis $(x_1, \ldots, x_{f+1})$ of A (the blanks in the matrix denote zeros). So α centralises x_{f+1} and if $1 \leq i \leq f$ then $x_i^{\alpha} = x_i x_{i+1}$. Now since $p \geq f + 1$ it follows that α

has order p and so if we denote by g an arbitrary generator of $C_{p^{n-f}}$ — the cyclic group of order p^{n-f} — then we can form the semi-direct product $P = A \rtimes C_{p^{n-f}}$ where g acts by α. P is therefore a group of order p^{n+1} which has coexponent $f+1$ and if $2 \leq i \leq f+2$ then the i-th term of the lower central series of P is the subgroup $\langle x_i, \ldots, x_{f+1} \rangle$, so that P has nilpotency class $f+1$. Now since $n - f \geq 2$ and g acts by an automorphism of order p, the element $g^{p^{n-f-1}}$ has order p and lies in the centre of P. Therefore $\langle g^{p^{n-f-1}} x_{f+1}^{-1} \rangle$ is a central subgroup of order p and the quotient

$$\overline{P} = {}^{P}\!/_{\langle g^{p^{n-f-1}} x_{f+1}^{-1} \rangle}$$

is a group of order p^n which has coexponent f and nilpotency class $f+1$. Note therefore, that if $p > f+1$ then $\overline{P}$ is also regular.

Notes.

i) Applying this example with $f = 2$, $n \geq 4$ and $p > 3$ shows that the bound in theorem 2·2 is attained for p-groups of coexponent 2 and that the restriction on the coexponent in theorem 3·2 was necessary.

ii) This example shows that for a fixed coexponent f there exist (regular) p-groups for arbitrarily large p which have coexponent f and nilpotency class exactly $f+1$ and this is the bound we seek for the second improvement.

Section 3·3. A Bound via Lie Rings.

In this section we aim to show that for each non-negative integer f there exists a cofinite set of primes $\mathcal{P}_f$ such that if P is a p-group of coexponent f with $p \in \mathcal{P}_f$ then $\mathrm{cl}(P) \leq f+1$ which, by the second note following the example in section 3·2, is the best one could hope for by excluding finitely many primes for each coexponent. In particular, we will show that $\mathcal{P}_f$ can be taken to be the set of primes greater than $2(f-1)$ for $f \geq 3$ (for $0 \leq f \leq 2$ we will take $\mathcal{P}_f$ to be the set of primes greater than $2f$). As mentioned in the introduction, we first prove the corresponding result for finite p-Lie rings and then use the functorial isomorphisms of section 1·1·3 to obtain the desired result. We first need an elementary analogy between groups and Lie rings.

In group theory, the **Frattini subgroup** $\Phi(G)$ of an arbitrary group G is defined to be the intersection of the maximal subgroups of G, and in the situation when G is a finite p-group it is straightforward to show that $\Phi(G) = G_2\mathfrak{U}_1(G)$ (see e.g. [14]). Moreover, we have the ***Burnside basis theorem*** which states that a subset Y of a finite p-group G is a generating set of G if and only if Y generates G modulo $\Phi(G)$, from which it follows that the number of elements in a minimal generating set of G is an invariant (denoted $d(G)$) which equals the dimension of the elementary Abelian p-group $G/\Phi(G)$ regarded as a vector space over $\mathbb{F}_p$ (again, see [14]). These results have a direct analogy for Lie rings as follows. If L is a Lie ring then we define the **Frattini subring** $\Phi(L)$ of L to be the intersection of the maximal subrings of L and the following result holds.

Proposition 3·3. *Let p be a prime number and L a finite nilpotent p-Lie ring. Then*

i) $\Phi(L)$ *is an ideal of* L *and* $\Phi(L) = L_2 + \mathfrak{U}_1(L)$.

ii) For a subset Y of L, Y generates L (as a Lie ring) if and only if Y generates L modulo $\Phi(L)$.

iii) The number of elements in a minimal generating set of L equals the dimension of the $\mathbb{F}_p$*–vector space* $L/\Phi(L)$.

The proof of this result is a direct modification of the corresponding group-theoretic results mentioned above and is therefore omitted.

If L is a finite p-Lie ring then we define the **coexponent** $f(L)$ of L in the obvious way to be the coexponent of the finite Abelian p-group $(L,+)$ so that, in particular, if L is in Λ_p then $f(L)$ coincides with the coexponent of the p-group $\mathcal{G}_p(L)$ (recall the results of section 1·1·3). We will now show the following result.

Theorem 3·4. *Let p be a prime and L a finite nilpotent p-Lie ring of coexponent $f(L)$. Then* $\mathrm{cl}(L) \leq f(L) + 1$.

Proof. If $f(L) = 0$ (i.e. $(L,+)$ is cyclic) then the result is clear, so we can suppose that $f(L) \geq 1$ which implies, in particular, that $(L,+)$ has at least two type invariants (i.e. $\omega_1(L) \geq 2$). So let L be of *type* $(\mu_1, \ldots, \mu_{\omega_1})$ (as defined in section 1·2), and recall that $\mu_1 \geq \mu_2 \geq \cdots \geq \mu_{\omega_1}$. It follows therefore that if $(u_1, \ldots, u_{\omega_1})$ is a basis of L corresponding

to the μ-invariants (i.e. u_i has order p^{μ_i} for each $i = 1, \ldots, \omega_1$), then

$$[p^{\mu_2} u_1, u_i] = 0 \text{ for each } i = 1, \ldots, \omega_1,$$

so that $p^{\mu_2} u_1$ is a central element of L. Also, the quotient Lie ring $L/\langle p^{\mu_2} u_1 \rangle$ is of *type* $(\mu_2(L), \mu_2(L), \mu_3(L), \ldots, \mu_{\omega_1}(L))$ and has coexponent $\sum_{i=2}^{\omega_1} \mu_i = f(L)$. So by factoring out by a central ideal (i.e. $\langle p^{\mu_2} u_1 \rangle$) we may assume that L is of *type* $(\mu_1, \mu_2, \ldots, \mu_{\omega_1})$ where $\mu_1 = \mu_2$, and the theorem will be proved if we can then show that $\mathrm{cl}(L) \leq f(L)$ under these hypotheses. This is what we now show.

If we let $(u_1, \ldots, u_{\omega_1})$ be a basis of L corresponding to the μ-invariants then we know from theorem 1·13 that $u_1, u_2, \ldots, u_{\omega_{\mu_1}}$ are the elements of the basis which have order p^{μ_1}, and so

$$L = \langle u_1 \rangle \oplus \langle u_2 \rangle \oplus \cdots \oplus \langle u_{\omega_{\mu_1}} \rangle \oplus S$$

where

$$S = \langle u_{\omega_{\mu_1}+1} \rangle \oplus \cdots \oplus \langle u_{\omega_1} \rangle,$$

and observe that $\omega_{\mu_1} \geq 2$ (by the hypothesis $\mu_1 = \mu_2$) and that the exponent of S is less than p^{μ_1}. Hence

$$\Omega_{\mu_1 - 1}(L) = \langle p u_1 \rangle \oplus \cdots \oplus \langle p u_{\omega_{\mu_1}} \rangle \oplus S,$$

and the quotient Lie ring $\overline{L}$ defined by

$$\overline{L} = L/\Omega_{\mu_1 - 1}(L)$$

has characteristic p and is therefore an ω_{μ_1}−dimensional nilpotent F_p−Lie algebra with a basis $(\overline{u}_1, \ldots, \overline{u}_{\omega_{\mu_1}})$ (where $\overline{u}_i = u_i + \Omega_{\mu_1 - 1}(L)$ for each $i = 1, \ldots, \omega_{\mu_1}$). Now since $\omega_{\mu_1}(L) \geq 2$ (by the assumption that $\mu_1(L) = \mu_2(L)$), it follows that $(\overline{L}, +)$ is not cyclic, and so by propostion 3·3 we have $|\overline{L} : \Phi(\overline{L})| \geq p^2$ which, since $[\overline{L}, \overline{L}] \subseteq \Phi(\overline{L})$, implies that $|\overline{L} : [\overline{L}, \overline{L}]| \geq p^2$. Therefore, $\overline{L}$ has an F_p−basis $(v_1, v_2, \ldots, v_{\omega_{\mu_1}})$ where $[\overline{L}, \overline{L}]$ is contained in the subspace spanned by $\{v_3, \ldots, v_{\omega_{\mu_1}}\}$. Now if we let $A = (\alpha_{ij})$ be an $(\omega_{\mu_1} \times \omega_{\mu_1})$ integer matrix with the property that

$$v_i = \sum_{j=1}^{\omega_{\mu_1}} \alpha_{ij} \overline{u}_j \text{ for each } i = 1, \ldots, \omega_{\mu_1},$$

then regarding $\overline{L}$ as an F_p−vector space, A mod p is the matrix of transition from $(v_1,\ldots,v_{\omega_{\mu_1}})$ to $(\overline{u}_1,\ldots,\overline{u}_{\omega_{\mu_1}})$. Therefore, A is invertible modulo p which implies that $\det(A)$ is coprime to p and so, in particular, A is invertible modulo p^{μ_1}. So since the subgroup F of L given by

$$F = \langle u_1\rangle \oplus \cdots \oplus \langle u_{\omega_{\mu_1}}\rangle$$

is a free $\mathbb{Z}/p^{\mu_1}\mathbb{Z}$−module with basis $(u_1,\ldots,u_{\omega_{\mu_1}})$, it follows that defining $(\tilde{u}_1,\ldots,\tilde{u}_{\omega_{\mu_1}})$ by

$$\tilde{u}_i = \sum_{j=1}^{\omega_{\mu_1}} \alpha_{ij}u_j \quad \text{for each} \quad i = 1,\ldots,\omega_{\mu_1},$$

gives a basis of F. Observe that for $1 \le i \le \omega_{\mu_1}$, the image of $\tilde{u}_i$ in $\overline{L}$ is v_i, and so since $[\overline{L},\overline{L}] \subseteq \langle v_3,\ldots,v_{\omega_{\mu_1}}\rangle$ it follows that for any $1 \le i,j \le \omega_{\mu_1}$ we have

$$[\tilde{u}_i,\tilde{u}_j] \in \langle \tilde{u}_3\rangle + \ldots + \langle \hat{u}_{\omega_{\mu_1}}\rangle + \Omega_{\mu_1-1}(L).$$

So using the fact that $\Omega_{\mu_1-1}(L) = \mathfrak{U}_1(F) \oplus S$ we see that

$$[F,F] \subseteq \langle p\hat{u}_1\rangle \oplus \langle p\tilde{u}_2\rangle \oplus \langle \tilde{u}_3\rangle \oplus \cdots \oplus \langle \tilde{u}_{\omega_{\mu_1}}\rangle \oplus S \tag{3·1}$$

and since S has exponent less than p^{μ_1} we also have

$$[F,S],\ [S,S] \subseteq \mathfrak{U}_1(F) \oplus S. \tag{3·2}$$

Now let $1 \le k \le \mu_1 - 1$ and consider the ideal

$$\left[\ {}^{\mathfrak{U}_k(L)}\!/_{\mathfrak{U}_{k+1}(L)}\ ,\ {}^{L}\!/_{\mathfrak{U}_{k+1}(L)}\ \right]$$

of the nilpotent p-Lie ring $L/\mathfrak{U}_{k+1}(L)$. From equations (3·1) and (3·2) it follows that

$$\left[\ \mathfrak{U}_k(L)\ ,\ L\ \right] \subseteq \langle p^{k+1}\hat{u}_1\rangle \oplus \langle p^{k+1}\hat{u}_2\rangle \oplus \langle p^k\tilde{u}_3\rangle \oplus \cdots \oplus \langle p^k\tilde{u}_{\omega_{\mu_1}}\rangle \oplus \mathfrak{U}_k(S)$$

which implies that

$$\left|\ {}^{\mathfrak{U}_k(L)}\!/_{\mathfrak{U}_{k+1}(L)}\ :\ \left[{}^{\mathfrak{U}_k(L)}\!/_{\mathfrak{U}_{k+1}(L)}\ ,\ {}^{L}\!/_{\mathfrak{U}_{k+1}(L)}\right]\ \right| \ \ge\ p^2 \tag{3·3}$$

Now if W is any finite nilpotent p-Lie ring and I is a non-zero ideal of W then we must have $|W : [I, W]| \geq p$, and so using the fact that

$$\left| \mathfrak{U}_k(L) : \mathfrak{U}_{k+1}(L) \right| = \left| \Omega_{k+1}(L) : \Omega_k(L) \right| = p^{\omega_{k+1}}$$

(an easy consequence of part (iv) of theorem 1·7), we see that for any i between 1 and $\omega_{k+1} - 1$ (inclusive), equation (3·3) implies that

$$\left| \mathfrak{U}_k(L)/\mathfrak{U}_{k+1}(L) \ : \ \left[\mathfrak{U}_k(L)/\mathfrak{U}_{k+1}(L) \ , \ \underbrace{L/\mathfrak{U}_{k+1}(L) \ , \ \cdots \ , \ L/\mathfrak{U}_{k+1}(L)}_{i \text{ times}} \right] \right| \geq p^{i+1}.$$

In particular, we have

$$\left[\mathfrak{U}_k(L) \ , \ \underbrace{L, \ \ldots \ , L}_{\substack{\omega_{k+1}-1 \\ \text{times}}} \right] \subseteq \mathfrak{U}_{k+1}(L) \ \text{ for each } \ k \ \text{ with } \ 1 \leq k \leq \mu_1 - 1. \qquad (3{\cdot}4)$$

Using this, we can now obtain the desired bound as follows. Since $L/\mathfrak{U}_1(L)$ is a nilpotent Lie ring of order p^{ω_1} and $\omega_1 > 1$ it is easy to see that $L_{\omega_1} \subseteq \mathfrak{U}_1(L)$, and then a straightforward inductive argument using this as the base case and equation (3·4) as the inductive step shows that for any i with $1 \leq i \leq \mu_1$, we have

$$L_{\omega_1 + \cdots + \omega_i - (i-1)} \subseteq \mathfrak{U}_i(L).$$

Applying this with $i = \mu_1$ shows us that $L_{n-\mu_1+1} = \{0\}$ (where $p^n = |L|$), and since $n - \mu_1 = f(L)$ we see that $L_{f(L)+1} = \{0\}$ which implies that $\mathrm{cl}(L) \leq f(L)$, as required. □

The following lemma is an easy consequence of this result and will enable us to prove the main theorem of this chapter.

Lemma 3·5. *Let P be a finite p-group of coexponent $f = f(P)$ and suppose that $\mathrm{cl}(P) < p$. Then $\mathrm{cl}(P) \leq f + 1$.*

Proof. Since P has nilpotency class less than p it belongs to the category Γ_p and so has an associated Lie ring structure $\mathcal{L}_p(P)$ defined on it (see section 1·1·3), and the coexponent of $\mathcal{L}_p(P)$ equals f. Therefore from theorem 3·4 we know that $\mathrm{cl}\big(\mathcal{L}_p(P)\big) \leq f + 1$ and so the lemma follows since P and $\mathcal{L}_p(P)$ have the same nilpotency class. □

Theorem 3·6. *For an integer f with $0 \leq f \leq 2$ let $\mathcal{P}_f$ be the set of primes greater than $2f$, and for an integer f greater than 2 let $\mathcal{P}_f$ be the set of primes greater than $2(f-1)$. Then if P is a finite p-group of coexponent $f = f(P)$ with $p \in \mathcal{P}_f$ it follows that* $\mathrm{cl}(P) \leq f + 1$.

Proof. Let P be a finite p-group of coexponent $f = f(P)$. If $f = 0$ then $\mathrm{cl}(P) = 1$ as required. If f is 1 or 2 with $p \in \mathcal{P}_f$ then p is an odd prime greater than $2f$ and so $\mathrm{cl}(P) < p$ (by theorem 2·1), from which it follows that $\mathrm{cl}(P) \leq f + 1$ by lemma 3·5. So suppose now that $f \geq 3$ (i.e. $f + 1 \leq 2(f-1)$), and let C denote a cyclic subgroup of index p^f in P. Then $|P : \mathfrak{U}_1(C)| = p^{f+1}$ which implies that $\omega(P) \leq f + 1$, and because p was chosen to be an element of $\mathcal{P}_f$ it follows that $\omega(P) < p$, i.e. P is absolutely regular. Therefore P is a regular p-group (by proposition 1·10), and so since we are assuming that $f \geq 3$, the bound given in theorem 3·2 applies so that $\mathrm{cl}(P) \leq 2(f-1)$. Hence P has nilpotency class less than p and so $\mathrm{cl}(P) \leq f + 1$ by lemma 3·5. □

Remark. This theorem has the consequence that if one is interested in looking at finite p-groups with a fixed coexponent $f \geq 3$, then by excluding the primes less than $2(f-1)$, the groups in question automatically have nilpotency class less than p and so belong to the category Γ_p. Therefore the Lie ring functors of section 1·1·3 can be used to study these groups, and this is the key observation for chapters 4 and 5. In particular, for $f = 3$ we only need to exclude the primes 2 and 3 to ensure that the Lie ring functors are applicable, and this is crucial to chapter 5.

Chapter 4. Regular p-Groups with a Fixed Coexponent

Section 4·1. Introduction.

For any prime p, the finite p-groups of coexponent 0,1 or 2 are understood. For coexponent 0 or 1 (the case of a cyclic maximal subgroup), [3] and [28] both contain a complete set of presentations, and Burnside's book [3] also contains presentations for the finite p-groups of coexponent 2 which possess a normal cyclic subgroup of index p^2. The remaining p-groups of coexponent 2 are discussed in Miller's paper [21] and a complete classification can be assembled by using his paper and the references he gives.

If, for a prime p and integers f and n with $1 \leq f < n$, we denote by $\Psi^p_{f,n}$ the number of groups of order p^n and coexponent f then the work of Burnside and Miller shows that for $f = 2$, $\Psi^p_{f,n}$ stabilises for p and n sufficiently large. In this chapter we investigate how $\Psi^p_{f,n}$ varies with p and n, for f an arbitrary fixed integer greater than 2. The main theorem we obtain is the following showing that for a fixed $f \geq 3$, $\Psi^p_{f,n}$ depends only on p, for p and n sufficiently large.

Theorem 4·1. *For an integer f greater than 2 and a prime number p greater than $2(f-1)$, we have*

$$\Psi^p_{f,n} = \Psi^p_{f,n'} \quad \textit{for} \quad n, n' \geq 3f.$$

We now discuss the method of proof after first introducing some notation.

Notation. Let p be any prime and suppose that $k \geq \lambda_1 \geq \cdots \geq \lambda_t$ are positive integers with $t \geq 1$. Then we denote by $\Psi^p_k(\lambda_1, \ldots, \lambda_t)$ the number of isomorphism classes of regular p-groups of *type* $(k, \lambda_1, \ldots, \lambda_t)$.

In the statement of the above theorem, the assumption $p > 2(f-1) \geq 4$ ensures that, by the proof of theorem 3·6, any p-group of coexponent f and order p^n (where n is greater than f) is (absolutely) regular and belongs to the category Γ_p. Therefore P is of

type$(n-f,\lambda_1,\ldots,\lambda_t)$ where $\underline{\lambda}=(\lambda_1,\ldots,\lambda_t)$ is a **partition** of f (i.e. $\lambda_1\geq\cdots\geq\lambda_t$ and $\sum_{i=1}^{t}\lambda_i=f$). Moreover, if $n>f$ and $\underline{\lambda}=(\lambda_1,\ldots,\lambda_t)$ is a partition of f with $n-f\geq\lambda_1$, then *any* regular p-group of *type*$(n-f,\lambda_1,\ldots,\lambda_t)$ has coexponent f and order p^n. We therefore have the following formula

$$\Psi^p_{f,n} \;=\; \sum_{\substack{\text{Partitions}\\ \underline{\lambda}\ \text{of}\ f\\ \text{with}\ n-f\geq\lambda_1}} \Psi^p_{n-f}(\underline{\lambda}) \qquad \text{for}\ \ n>f\geq 3\ \ \text{and}\ \ p>2(f-1),$$

and so by assuming that $n\geq 2f\geq 6$ we obtain

$$\Psi^p_{f,n} \;=\; \sum_{\substack{\text{Partitions}\\ \underline{\lambda}\ \text{of}\ f}} \Psi^p_{n-f}(\underline{\lambda}) \qquad \text{for}\ \ n\geq 2f\geq 6\ \ \text{and}\ \ p>2(f-1). \tag{4·1}$$

So to prove theorem 4·1 it suffices to study the behaviour of the function $\Psi^p_k(\lambda_1,\ldots,\lambda_t)$ as k varies. Now since any regular p-group P of *type*$(k,\lambda_1,\ldots,\lambda_t)$ where $k\geq\lambda_1\geq\cdots\geq\lambda_t$ and $p>2(\sum_{i=1}^{t}\lambda_i-1)\geq 4$ belongs to the category Γ_p, it has an associated Lie ring $\mathcal{L}_p(P)$ in Λ_p which is also of *type*$(k,\lambda_1,\ldots,\lambda_t)$. Moreover, since the functor $\mathcal{L}_p$ gives an isomorphism between the categories Γ_p and Λ_p, it follows that $\Psi^p_k(\lambda_1,\ldots,\lambda_t)$ equals the number of isomorphism classes of Lie rings in Λ_p of *type*$(k,\lambda_1,\ldots,\lambda_t)$, and so the function $\Psi^p_k(\lambda_1,\ldots,\lambda_t)$ can be studied by looking at the corresponding Lie rings. This is the approach we will take in section 4·3, and in section 4·4 we reinterpret the results in terms of regular p-groups with the ultimate aim of proving theorem 4·1. The proofs of the results in section 4·3 are constructive in nature and will be used (and illustrated) to good effect in the next chapter where we consider the groups of order p^n and coexponent 3 for $p\geq 5$ and $n\geq 7$. We will calculate $\Psi^p_{n-3}(2,1)$ and $\Psi^p_{n-3}(3)$ explicitly, and using a theorem to be proved in this chapter (theorem 4·10) we reduce the calculation of $\Psi^p_{n-3}(1,1,1)$ to the known classification of groups of order p^3. Assuming this classification therefore, equation (4·1) gives us a formula for the number of groups of order p^n and coexponent 3 for $p\geq 5$ and $n\geq 7$.

Section 4·2. Preliminaries on Derivations.

In this section we recall the notion of a derivation and how they are used to construct split extensions of Lie algebras. We will be using this construction in the next section in the context of Lie rings.

Let C be a commutative ring with 1 and suppose that A is a C-algebra (not necessarily associative — recall the definitions in section 1·1·1). A **derivation** of A is defined to be a C-linear map $\sigma : A \to A$ which satisfies the property

$$[x,y]\,\sigma = [x\sigma, y] + [x, y\sigma] \quad \text{for each} \quad x, y \in A, \tag{4·2}$$

and it is easy to see that the set of derivations $\mathrm{Der}(A)$ of A forms a C-submodule of the associative algebra $\mathrm{End}_C(A)$ (we will write maps on the right). Moreover, since $\mathrm{End}_C(A)$ is associative it has an associated C-Lie algebra structure $\mathrm{End}_C(A)_L$ (see section 1·1·1) and it is a routine matter to check that $\mathrm{Der}(A)$ is a Lie subalgebra of $\mathrm{End}_C(A)_L$. We will refer to $\mathrm{Der}(A)$ as the **derivation algebra** of A.

Given an element x of A, we define two C-linear maps $\mathrm{ad}_l x$ and $\mathrm{ad}_r x$ by

$$\begin{array}{rcccc} \mathrm{ad}_l x & : & A & \longrightarrow & A \\ & : & y & \longmapsto & [x,y] \end{array} \qquad \text{and} \qquad \begin{array}{rcccc} \mathrm{ad}_r x & : & A & \longrightarrow & A \\ & : & y & \longmapsto & [y,x] \end{array}$$

called the left and right adjoint maps of x, respectively. In this context, the Jacobi identity holds in A if and only if $\mathrm{ad}_r x \in \mathrm{Der}(A)$ for each element x of A. So if A is a C-Lie algebra then the right adjoint maps are derivations of A and since the Lie bracket is skew-symmetric it follows that $\mathrm{ad}_l x \in \mathrm{Der}(A)$ for any $x \in A$. A derivation σ of a C-Lie algebra A is called an **inner derivation** of A if $\sigma = \mathrm{ad}_r x$ for some $x \in A$, and it is easy to see that the set of inner derivations $\mathrm{Inn}(A)$ is an ideal of the derivation algebra $\mathrm{Der}(A)$ by using the fact that for any $x, y \in A$ and $\tau \in \mathrm{Der}(A)$ we have

$$y\,[\mathrm{ad}_r x, \tau] = y\big((\mathrm{ad}_r x)\tau - \tau(\mathrm{ad}_r x)\big) = y\,\mathrm{ad}_r(x\tau).$$

A non-inner derivation of A is referred to as an **outer derivation** of A and the quotient Lie algebra $\mathrm{Der}(A)/\mathrm{Inn}(A)$ is called the **outer derivation algebra** of A, denoted $\mathrm{Out}(A)$.

The terminology used here suggesting a connection between inner and outer automorphisms of a group is deliberate and indicates the appropriate manner in which to define split extensions of Lie algebras. Given two C-Lie algebras L and M we understand a **(right) action** of M on L to mean a homomorphism of C-Lie algebras $\theta : M \to \mathrm{Der}(L)$, and denoting the Lie brackets on L and M by $[.,.]_L$ and $[.,.]_M$ respectively, we use such an action to define a C-Lie algebra $L \rtimes_\theta M$ as follows. The underlying C-module of $L \rtimes_\theta M$ is the direct sum $L \oplus M$ and, identifying L and M with the natural submodules of $L \oplus M$, we define the bracket of $l_1 + m_1, l_2 + m_2 \in L \oplus M$ by

$$[l_1 + m_1 , l_2 + m_2] = [l_1, l_2]_L + l_1(m_2\theta) - l_2(m_1\theta) + [m_1, m_2]_M. \qquad (4{\cdot}3)$$

The verification that this does indeed define a C-Lie bracket is routine and need not be reproduced here. It is then straightforward to see that, under the natural identifications, $L \rtimes_\theta M$ is a split extension of L by M where if $m \in M$ then the restriction of $\mathrm{ad}_r m$ to L is precisely the derivation $m\theta$.

Analogous to the semi-direct product of groups, the C-Lie algebra $L \rtimes_\theta M$ is characterised by a universal property. Let N be a C-Lie algebra which is the sum of an ideal L' and a subalgebra M' and suppose that there exists isomorphisms of C-Lie algebras $\phi : L \to L'$, $\varphi : M \to M'$ such that the following diagram commutes

$$\begin{array}{ccc} \mathrm{Der}(L) & \xrightarrow{\overline{\phi}} & \mathrm{Der}(L') \\ {\scriptstyle\theta}\uparrow & & \uparrow{\scriptstyle\nu} \\ M & \xrightarrow[\varphi]{} & M' \end{array}$$

where $\overline{\phi}$ is the isomorphism of derivation algebras induced by ϕ (i.e. $\sigma\overline{\phi} = \phi^{-1}\sigma\phi$ for a derivation σ of L), and $m'\nu = \mathrm{ad}_r m'|_{L'}$ for $m' \in M'$. Then it follows easily from equation (4·3) that there exists a ***unique*** epimorphism of C-Lie algebras $\gamma : L \rtimes_\theta M \twoheadrightarrow N$ with $\gamma|_L = \phi$ and $\gamma|_M = \varphi$.

A derivation σ of a C-Lie algebra L is said to **centralise** an element u of L if $u\sigma = 0$, and we denote by $\mathrm{Der}(L)_u$ the collection of all derivations centralising u which is easily seen to be a subalgebra of $\mathrm{Der}(L)$.

A derivation σ of a C-Lie algebra L is called **nilpotent** if there exists some natural number k with the property that $\sigma^k = 0$, and an action θ of a C-Lie algebra M on L is

called **nil** if $m\theta$ is nilpotent for each $m \in M$. If L is a nilpotent C-Lie algebra then it is easy to see that the adjoint map $\mathrm{ad} : L \to \mathrm{Der}(L)$ is a nil action of L on itself (the fact that ad is an action follows from the Jacobi identity). In the case that C is a field this observation has a famous converse known as ***Engel's theorem*** which states that if the adjoint map of a finite-dimensional Lie algebra L is nil then L is nilpotent. The proof of this theorem can be found in any standard textbook (see e.g. [11]), although we will only be needing the following result which is the Lie ring analogue of a result which can be used to prove Engel's theorem (the proof of this result is from a lecture course on Lie Algebras given by R.W. Carter).

Lemma 4·2. *Let L be a Lie ring and suppose that $L = I + \langle u \rangle$ where I is a nilpotent ideal and $\mathrm{ad}_r u$ is nilpotent. Then L is nilpotent.*

Proof (sketch). The result will follow if we can show that for any natural number j there exists another natural number n_j such that $L_{n_j} \subseteq I_j$. The case $j = 1$ is clear since L/I is Abelian, so suppose inductively that we have shown it for some $j \geq 1$. It then follows that $L_{n_j+1} \subseteq I_{j+1} + L_{n_j}\mathrm{ad}_r u$. Using this as the base case for a second induction, it is straightforward to show that $L_{n_j+k} \subseteq I_{j+1} + L_{n_j}(\mathrm{ad}_r u)^k$ for any $k \geq 1$. Nilpotency of $\mathrm{ad}_r u$ then implies that $L_{n_j+k} \subseteq I_{j+1}$ for some $k \in \mathbb{N}$, as required. □

Section 4·3. Finite p-Lie Rings with a Fixed Coexponent.

For a prime p and positive integers $k, \lambda_1, \ldots, \lambda_t$ where $t \geq 1$ and $k \geq \lambda_1 \geq \cdots \geq \lambda_t$, we will denote by $\mathcal{F}_k^p(\lambda_1, \ldots, \lambda_t)$ the collection of all finite p-Lie rings L of *type* $(k, \lambda_1, \ldots, \lambda_t)$ (i.e. the $\mu-$invariants of L satisfy $\mu_1(L) = k$, $\mu_{1+i}(L) = \lambda_i$ for $i = 1, \ldots, t$, and $\omega_1(L) = 1 + t$). Observe that the coexponent of a Lie ring in $\mathcal{F}_k^p(\lambda_1, \ldots, \lambda_t)$ is $\sum_{i=1}^t \lambda_i$ and so is fixed for the whole family. The number of isomorphism classes in $\mathcal{F}_k^p(\lambda_1, \ldots, \lambda_t)$ will be denoted by $\Upsilon_k^p(\lambda_1, \ldots, \lambda_t)$ and we will show the following theorem.

Theorem 4·3. *For $k, k' \geq 2\lambda_1$ we have $\Upsilon_k^p(\lambda_1, \ldots, \lambda_t) = \Upsilon_{k'}^p(\lambda_1, \ldots, \lambda_t)$.*

To show this, we first observe that if $k \geq 2\lambda_1$ and L is in $\mathcal{F}_k^p(\lambda_1, \ldots, \lambda_t)$ with a basis $(h, g_1, \ldots, g_t)$ corresponding to the type invariants of L, then

$$\Omega_{\lambda_1}(L) = \langle p^{k-\lambda_1} h \rangle \oplus \langle g_1 \rangle \oplus \cdots \oplus \langle g_t \rangle$$

with $p^{k-\lambda_1} h \in Z(L)$. So denoting $\Omega_{\lambda_1}(L)$ by U we then see that U is a Lie ring with the following properties :

1. $|U| = p^{\lambda_1 + f}$ where $f = \sum_{i=1}^{t} \lambda_i$.
2. U is of *type* $(\lambda_1, \lambda_1, \lambda_2, \ldots, \lambda_t)$.
3. U has a basis $(z, u_1, \ldots, u_t)$ corresponding to its type invariants where $z \in Z(U)$.

(4·4)

Now if U is *any* Lie ring satisfying the properties (4·4) then for $k \geq 2\lambda_1$ we denote by $\Upsilon_k^p(\lambda_1, \ldots, \lambda_t, U)$ the number of isomorphism classes of Lie rings L in $\mathcal{F}_k^p(\lambda_1, \ldots, \lambda_t)$ with $\Omega_{\lambda_1}(L) \cong U$ (this is well-defined since $L \cong M$ implies that $\Omega_{\lambda_1}(L) \cong \Omega_{\lambda_1}(M)$), and then taking $\mathcal{U}^p(\lambda_1, \ldots, \lambda_t)$ to be an arbitrary transversal for the isomorphism classes of Lie rings satisfying (4·4) it follows that

$$\Upsilon_k^p(\lambda_1, \ldots, \lambda_t) = \sum_{U \in \mathcal{U}^p(\lambda_1, \ldots, \lambda_t)} \Upsilon_k^p(\lambda_1, \ldots, \lambda_t, U) \qquad \text{for } k \geq 2\lambda_1. \tag{4·5}$$

So to prove theorem 4·3 it suffices to show the following result.

Theorem 4·4. *Let U satisfy (4·4) and suppose that $k, k' \geq 2\lambda_1$. Then*

$$\Upsilon_k^p(\lambda_1, \ldots, \lambda_t, U) = \Upsilon_{k'}^p(\lambda_1, \ldots, \lambda_t, U).$$

Proof. Fix $k \geq 2\lambda_1$ and a basis $(z, u_1, \ldots, u_t)$ of U as asserted by property 3 of (4·4). Now suppose that L is in $\mathcal{F}_k^p(\lambda_1, \ldots, \lambda_t)$ with $\phi : U \to \Omega_{\lambda_1}(L)$ an isomorphism of Lie rings, and let $(h, g_1, \ldots, g_t)$ be a basis of L corresponding to its type invariants. As above, $p^{k-\lambda_1}h$ is a central element of L of order p^{λ_1}, and so $(p^{k-\lambda_1}h)\phi^{-1}$ is a central element of U of order p^{λ_1}.

We can therefore assume that $z\phi = p^{k-\lambda_1}h$, and we denote by $\overline{\phi}$ the induced isomorphism

$$\begin{array}{rccc} \overline{\phi} & : & \mathrm{Der}(U)_z & \longrightarrow & \mathrm{Der}\big(\Omega_{\lambda_1}(L)\big)_{p^{k-\lambda_1}h} \\ & & \sigma & \longmapsto & \phi^{-1}\sigma\phi \end{array}$$

Since $\Omega_{\lambda_1}(L)$ is an ideal of L we see that $\tau = \mathrm{ad}_r h|_{\Omega_{\lambda_1}(L)}$ belongs to $\mathrm{Der}\big(\Omega_{\lambda_1}(L)\big)_{p^{k-\lambda_1}h}$ and if we let σ be the derivation $\phi\tau\phi^{-1}$ then $\sigma \in \mathrm{Der}(U)_z$ and $\sigma\overline{\phi} = \tau$. Now because U has additive exponent p^{λ_1} it follows that $\mathrm{Der}(U)$ has additive exponent dividing p^{λ_1} and therefore fixing an arbitrary generator e_k of the Abelian Lie ring $\mathbf{Z}/p^k\mathbf{Z}$ (all brackets 0 — the only possibility), we have a commutative diagram of Lie rings

$$\begin{array}{ccc} \mathrm{Der}(U)_z & \xrightarrow{\ \overline{\phi}\ } & \mathrm{Der}\big(\Omega_{\lambda_1(L)}\big)_{p^{k-\lambda_1}h} \\ {\scriptstyle\theta}\uparrow & & \uparrow{\scriptstyle\nu} \\ \big(\mathbf{Z}/_{p^k\mathbf{Z}}\big)e_k & \underset{\varphi}{\longrightarrow} & \langle h \rangle \end{array}$$

where $e_k\theta = \sigma$, $e_k\varphi = h$ and $h\nu = \tau$. Hence, by the discussion in section 4·2, we have a Lie ring epimorphism

$$\gamma \ : \ U \rtimes_\theta \big(\mathbf{Z}/_{p^k\mathbf{Z}}\big)e_k \quad \longrightarrow \quad L$$

where $\gamma|_U = \phi$, $e_k\gamma = h$ and $\ker(\gamma) = \langle z - p^{k-\lambda_1}e_k \rangle$.

Conversely, if z is *any* central element of U of order p^{λ_1}, σ is any element of $\mathrm{Der}(U)_z$, and $\theta : (\mathbf{Z}/p^k\mathbf{Z})e_k \to \mathrm{Der}(U)_z$ is the (unique) Lie ring epimorphism with $e_k\theta = \sigma$ then the subgroup $\langle z - p^{k-\lambda_1}e_k \rangle$ is a central ideal of $U \rtimes_\theta (\mathbf{Z}/p^k\mathbf{Z})e_k$ (using the fact that $k \geq 2\lambda_1$ and e_k centralises z) with the quotient

$$U^\sigma_{z,e_k} \quad = \quad U \rtimes_\theta (\mathbf{Z}/p^k\mathbf{Z})e_k \ \Big/ \langle z - p^{k-\lambda_1}e_k \rangle \qquad (\text{where } e_k\theta = \sigma) \qquad (4\cdot6)$$

belonging to $\mathcal{F}_k^p(\lambda_1,\ldots,\lambda_t)$ and

$$\Omega_{\lambda_1}(U^{\sigma}_{z,e_k}) \quad = \quad U + \langle z - p^{k-\lambda_1}e_k\rangle \Big/ \langle z - p^{k-\lambda_1}e_k\rangle \tag{4·7}$$

is (naturally) isomorphic to U (since $U \cap \langle z - p^{k-\lambda_1}e_k\rangle = \{0\}$). Therefore, we have shown that for $k \geq 2\lambda_1$, $\Upsilon_k^p(\lambda_1,\ldots,\lambda_t,U)$ equals the number of isomorphism classes arising from the set of Lie rings

$$T(U,k,e_k) \quad = \bigcup_{\substack{z\in U \\ \text{central of order } p^{\lambda_1}}} T(U,k,z,e_k),$$

where for $z \in U$ central of order p^{λ_1} we define

$$T(U,k,z,e_k) \;=\; \{\, U^{\sigma}_{z,e_k} \;:\; \sigma \in \mathrm{Der}(U)_z\}. \tag{4·8}$$

This observation and the following lemma will enable us to complete the proof of theorem 4·4.

Lemma 4·5. *Suppose $k \geq 2\lambda_1$, and $z, z' \in U$ are central elements of order p^{λ_1}. If $\sigma \in \mathrm{Der}(U)_z$ and $\tau \in \mathrm{Der}(U)_{z'}$ then*

U^{σ}_{z,e_k} is isomorphic to U^{τ}_{z',e_k} if and only if there exists $\pi \in \mathrm{Aut}_{\mathrm{Lie}}(U)$ with

i) $z\pi = \alpha z'$ for some $\alpha \in \mathbb{Z}$ with $(\alpha,p) = 1$.
ii) $\pi^{-1}\sigma\pi = \mathrm{ad}_r x + \alpha\tau$ for some $x \in U$.

Proof. Suppose first that $U^{\sigma}_{z,e_k} \cong U^{\tau}_{z',e_k}$ and let $\eta : U^{\sigma}_{z,e_k} \to U^{\tau}_{z',e_k}$ be a Lie ring isomorphism. Now by equation (4·7) we can identify U with the ideals $\Omega_{\lambda_1}(U^{\sigma}_{z,e_k})$ and $\Omega_{\lambda_1}(U^{\tau}_{z',e_k})$ of U^{σ}_{z,e_k} and U^{τ}_{z',e_k} respectively, and with this identification, U is invariant under η and so $\eta|_U \in \mathrm{Aut}_{\mathrm{Lie}}(U)$. Now since η is an Abelian group homomorphism, we must have $e_k\eta = x + \alpha e_k$ for some $x \in U$ and $\alpha \in \mathbb{Z}$ with $(\alpha, p) = 1$, and then $z\eta = (p^{k-\lambda_1}e_k)\eta = p^{k-\lambda_1}(e_k\eta) = \alpha z'$. If we now let $[.,.]_\sigma$ and $[.,.]_\tau$ be the Lie brackets on U^{σ}_{z,e_k} and U^{τ}_{z',e_k} respectively, then for any $w \in U$ we have

$$w\,(\eta|_U{}^{-1}\sigma\,\eta|_U) \;=\; [w\eta^{-1}, e_k]_\sigma\,\eta \;=\; [w, e_k\eta]_\tau \;=\; w(\mathrm{ad}_r x + \alpha\tau).$$

Therefore conditions i) and ii) hold with $\pi = \eta|_U$.

Conversely, suppose that there exists $\pi \in \mathrm{Aut}_{\mathrm{Lie}}(U)$ satisfying conditions i) and ii). Define a homomorphism χ of Abelian groups by

$$\begin{array}{rccc} \chi \;:\; U \oplus \left(\mathbb{Z}/p^k\mathbb{Z}\right)e_k & \longrightarrow & U \oplus \left(\mathbb{Z}/p^k\mathbb{Z}\right)e_k \\ w & \longmapsto & w\pi, \quad w \in U \\ e_k & \longmapsto & x + \alpha e_k \end{array}$$

and observe that the condition $(\alpha, p) = 1$ ensures that $\chi \in \mathrm{Aut}_{\mathbb{Z}}(U \oplus (\mathbb{Z}/p^k\mathbb{Z})e_k)$. Let $\theta : (\mathbb{Z}/p^k\mathbb{Z})e_k \to \mathrm{Der}(U)_z$, and $\theta' : (\mathbb{Z}/p^k\mathbb{Z})e_k \to \mathrm{Der}(U)_{z'}$ be the Lie ring homomorphisms where $e_k\theta = \sigma$ and $e_k\theta' = \tau$, and denote by $[.,.]_\sigma$ and $[.,.]_\tau$ the Lie brackets giving rise to $U \rtimes_\theta (\mathbb{Z}/p^k\mathbb{Z})e_k$ and $U \rtimes_{\theta'} (\mathbb{Z}/p^k\mathbb{Z})e_k$, respectively. Then for any $w \in U$ we see that

$$[w, e_k]_\sigma\,\chi \;=\; (w\sigma)\chi \;=\; (w\sigma)\pi \;=\; [w\pi, e_k\chi]_\tau \;=\; [w\chi, e_k\chi]_\tau,$$

from which it follows that χ is a Lie ring isomorphism

$$U \rtimes_\theta \left(\mathbb{Z}/p^k\mathbb{Z}\right)e_k \quad\longrightarrow\quad U \rtimes_{\theta'} \left(\mathbb{Z}/p^k\mathbb{Z}\right)e_k.$$

Since we also have

$$\langle z - p^{k-\lambda_1}e_k\rangle\chi \;=\; \langle \alpha\,(z' - p^{k-\lambda_1}e_k)\rangle \;=\; \langle z' - p^{k-\lambda_1}e_k\rangle,$$

it follows therefore that χ induces a Lie ring isomorphism $\overline{\chi} : U^{\sigma}_{z,e_k} \to U^{\tau}_{z',e_k}$, as required. □

To complete the proof of theorem 4·4 we merely observe that conditions i) and ii) in the statement of lemma 4·5 are independent of k, and so for $k, k' \geq 2\lambda_1$ the number of isomorphism classes arising from $T(U, k, e_k)$ and $T(U, k', e_{k'})$ are equal, i.e. $\Upsilon_k^p(\lambda_1, \ldots, \lambda_t, U) = \Upsilon_{k'}^p(\lambda_1, \ldots, \lambda_t, U)$, and this completes the proof of theorem 4·4. □

Since $\mathcal{F}_k^p(\lambda_1, \ldots, \lambda_t)$ consists of ***all*** finite p-Lie rings of ***type*** $(\lambda_1, \ldots, \lambda_t)$ with no assumption of nilpotency, we need to show that by restricting attention to the isomorphism classes of nilpotent Lie rings in $\mathcal{F}_k^p(\lambda_1, \ldots, \lambda_t)$ analogous results to theorems 4·3 and 4·4 hold. These results will follow easily from an examination of the proof of theorem 4·4 after introducing some more notation.

So for $k \geq \lambda_1 \geq \cdots \geq \lambda_t$ let $\Delta_k^p(\lambda_1, \ldots, \lambda_t)$ denote the number of isomorphism classes of nilpotent Lie rings in $\mathcal{F}_k^p(\lambda_1, \ldots \lambda_t)$. Now if $k \geq 2\lambda_1$ and L is a nilpotent Lie ring in $\mathcal{F}_k^p(\lambda_1, \ldots \lambda_t)$ then $\Omega_{\lambda_1}(L)$ is a ***nilpotent*** Lie ring satisfying (4·4). Therefore if, for an arbitrary nilpotent Lie ring U satisfying (4·4) and $k \geq 2\lambda_1$, we denote by $\Delta_k^p(\lambda_1, \ldots, \lambda_t, U)$ the number of isomorphism classes of nilpotent Lie rings L in $\mathcal{F}_k^p(\lambda_1, \ldots \lambda_t)$ with $\Omega_{\lambda_1}(L) \cong U$, then taking $\mathcal{N}^p(\lambda_1, \ldots, \lambda_t)$ to be an arbitrary transversal for the nilpotent Lie rings satisfying (4·4) we have

$$\Delta_k^p(\lambda_1, \ldots, \lambda_t) = \sum_{U \in \mathcal{N}^p(\lambda_1, \ldots, \lambda_t)} \Delta_k^p(\lambda_1, \ldots, \lambda_t, U) \quad \text{for } k \geq 2\lambda_1 \tag{4·9}$$

We now have the following result

Theorem 4·6. *Let $\lambda_1 \geq \cdots \geq \lambda_t$ be positive integers.*

i) If U is a nilpotent Lie ring satisfying (4·4) then for $k, k' \geq 2\lambda_1$ we have $\Delta_k^p(\lambda_1, \ldots, \lambda_t, U) = \Delta_{k'}^p(\lambda_1, \ldots, \lambda_t, U)$.

ii) $\Delta_k^p(\lambda_1, \ldots, \lambda_t) = \Delta_{k'}^p(\lambda_1, \ldots, \lambda_t)$ for $k, k' \geq 2\lambda_1$.

Proof.

i) Let $k \geq 2\lambda_1$. Recall from equation (4·8) the definition of $T(U,k,e_k)$ and observe that $\Delta_k^p(\lambda_1,\ldots,\lambda_t,U)$ is the number of isomorphism classes of nilpotent Lie rings in $T(U,k,e_k)$. Now if $U^\sigma_{z,e_k} \in T(U,k,e_k)$ is nilpotent then identifying e_k and U with their natural images in U^σ_{z,e_k} we see that

$$U^\sigma_{z,e_k} = U + \langle e_k \rangle$$

and since $\mathrm{ad}_r e_k|_U = \sigma$ we see that σ is a nilpotent element of $\mathrm{Der}(U)_z$. Conversely, if z is a central element of U of order p^{λ_1} and if $\sigma \in \mathrm{Der}(U)_z$ is nilpotent then U^σ_{z,e_k} is nilpotent by lemma 4·2. Hence $\Delta_k^p(\lambda_1,\ldots,\lambda_t,U)$ is the number of isomorphism classes arising from the set

$$N(U,k,e_k) = \bigcup_{\substack{z \in U \\ \text{central of order } p^{\lambda_1}}} N(U,k,z,e_k),$$

where for $z \in U$ central of order p^{λ_1} we define

$$N(U,k,z,e_k) = \left\{ U^\sigma_{z,e_k} \,:\, \sigma \text{ a nilpotent element of } \mathrm{Der(U)}_z \right\},$$

and this number is independent of $k \geq 2\lambda_1$ by lemma 4·5.

ii) This follows immediately from i) and equation (4·9). □

Corollary 4·7. *For an integer $c \geq 1$, the number of isomorphism classes of nilpotent Lie rings L in $\mathcal{F}_k^p(\lambda_1,\ldots,\lambda_t)$ with $\mathrm{cl}(L) = c$ is independent of $k \geq 2\lambda_1$.*

Proof. Let U be a nilpotent Lie ring satisfying (4·4) and suppose that $k, k' \geq 2\lambda_1$. Then by the proof of theorem 4·6 we have a bijection

$$\begin{array}{ccc} N(U,k,e_k) & \longrightarrow & N(U,k',e_{k'}) \\ U^\sigma_{z,e_k} & \longmapsto & U^\sigma_{z,e_{k'}} \end{array}$$

inducing a one-to-one correspondence between isomorphism classes. The result will follow immediately if we can show that the nilpotency class is also preserved. So let $z \in U$ be a central element of order p^{λ_1} and let σ be a nilpotent element of $\mathrm{Der}(U)_z$. Identifying U with the natural ideals of U^σ_{z,e_k} and $U^\sigma_{z,e_{k'}}$ we see that

$$\gamma_2(U^\sigma_{z,e_k}) = [U,U] + U\sigma = \gamma_2(U^\sigma_{z,e_{k'}}),$$

and then an easy induction shows that

$$\gamma_{r+1}(U^{\sigma}_{z,e_k}) = \gamma_{r+1}(U^{\sigma}_{z,e_{k'}}), \quad r \geq 2,$$

and so the nilpotency class is preserved. □

Section 4·4. Interpreting the Results for Regular p-Groups.

In this section we use the isomorphism between the categories Γ_p and Λ_p to recast the main results in the previous section concerning nilpotent Lie rings in terms of regular p-groups. Theorem 4·1 will then follow immediately from these results. In this section $\lambda_1, \ldots, \lambda_t$ will denote fixed positive integers where $\lambda_1 \geq \cdots \geq \lambda_t$ and $t \geq 1$, and k will denote a variable positive integer greater than or equal to λ_1. We then have the following result.

Proposition 4·8. *For any prime p and an integer c with $1 \leq c < p$, the number of isomorphism classes of regular p-groups P of type $(k, \lambda_1, \ldots, \lambda_t)$ with $\mathrm{cl}(P) = c$ is independent of $k \geq 2\lambda_1$.*

Proof. If P is such a group then P is in Γ_p (since $c < p$) and then the Lie ring $\mathcal{L}_p(P)$ is a nilpotent Lie ring in $\mathcal{F}^p_k(\lambda_1, \ldots, \lambda_t)$ with $\mathrm{cl}(\mathcal{L}_p(P)) = c$. Conversely, if L is a nilpotent Lie ring in $\mathcal{F}^p_k(\lambda_1, \ldots, \lambda_t)$ with $\mathrm{cl}(L) = c$ then L is in Λ_p and the group $\mathcal{G}_p(L)$ is a regular p-group of *type* $(k, \lambda_1, \ldots, \lambda_t)$ with $\mathrm{cl}(\mathcal{G}_p(L)) = c$. The result therefore follows from corollary 4·7 and the fact that $\mathcal{L}_p$ and $\mathcal{G}_p$ are mutually inverse isomorphisms. □

The following corollary is immediate from this result.

Corollary 4·9. *For a prime p the number of isomorphism classes of p-groups in Γ_p of type $(k, \lambda_1, \ldots, \lambda_t)$ is independent of $k \geq 2\lambda_1$.* □

We now use the results of chapter 3 to restrict the primes p which are considered in order to prove theorem 4·1.

Theorem 4·10. *Let* $p > 2(\sum_{i=1}^{t} \lambda_i - 1)$ *and suppose that* $\sum_{i=1}^{t} \lambda_i \geq 3$. *Then*

i) $\Psi_k^p(\lambda_1, \ldots, \lambda_t) = \Delta_k^p(\lambda_1, \ldots, \lambda_t)$ for $k \geq \lambda_1$.

ii) $\Psi_k^p(\lambda_1, \ldots, \lambda_t) = \Psi_{k'}^p(\lambda_1, \ldots, \lambda_t)$ for $k, k' \geq 2\lambda_1$.

Proof.

i) Let $f = \sum_{i=1}^{t} \lambda_i$ and observe that the conditions imply that $f + 1 \leq 2(f-1) < p$. Now if P is a regular p-group of *type* $(k, \lambda_1, \ldots, \lambda_t)$ then by theorem 3·6 we know that P is in Γ_p and so $\mathcal{L}_p(P)$ is a nilpotent Lie ring in $\mathcal{F}_k^p(\lambda_1, \ldots, \lambda_t)$. Conversely, if L is a nilpotent Lie ring in $\mathcal{F}_k^p(\lambda_1, \ldots, \lambda_t)$ then $\mathrm{cl}(L) \leq f + 1$ by theorem 3·4 and therefore L is in Λ_p and $\mathcal{G}_p(L)$ is of *type* $(k, \lambda_1, \ldots, \lambda_t)$. The result then follows since the functors $\mathcal{L}_p$ and $\mathcal{G}_p$ preserve isomorphism.

ii) This follows immediately from i) and the second part of theorem 4·6. □

We conclude this section by using this result to prove theorem 4·1 which was stated in the introduction to this chapter.

Proof of Theorem 4·1.

Let $f \geq 3$ and $p > 2(f-1)$. Now if $n, n' \geq 3f$ and $\underline{\lambda} = (\lambda_1, \ldots, \lambda_t)$ is a partition of f then we have $n - f$, $n' - f \geq 2f \geq 2\lambda_1$ and $p > 2(\sum_{i=1}^{t} \lambda_i - 1)$, Hence by theorem 4·10 we have $\Psi_{n-f}^p(\underline{\lambda}) = \Psi_{n'-f}^p(\underline{\lambda})$ and so using equation (4·1) we have

$$\Psi_{f,n}^p = \sum_{\substack{\text{Partitions} \\ \underline{\lambda} \text{ of } f}} \Psi_{n-f}^p(\underline{\lambda}) = \sum_{\substack{\text{Partitions} \\ \underline{\lambda} \text{ of } f}} \Psi_{n'-f}^p(\underline{\lambda}) = \Psi_{f,n'}^p$$

which completes the proof. □

Chapter 5. Finite p-Groups of Coexponent 3

Section 5·1. Introduction.

In the introduction to the last chapter it was mentioned that the groups of order p^n and coexponent at most 2 were classified at around the turn of the century by Burnside [3] and Miller [21]. In this chapter we consider the groups of coexponent 3 and produce a formula for the number of groups of order p^n and coexponent 3 for $p \geq 5$ and $n \geq 7$. The formula we give relies in part on the known classification of groups of order p^5 for $p \geq 5$ of which the most recent list is given in [12]. The fact that we can reduce some of the calculations to this known classification is due to **theorem 4·10** of the previous chapter. Recalling the notation of the previous chapter, the majority of this chapter is devoted to showing the following result

Lemma 5·1. *Let p be a prime greater than or equal to 5. Then*

i) $\Psi^p_{n-3}(1,1,1) = 23 + 2(p-1,3) + (p-1,4), \quad n \geq 5.$

ii) $\Psi^p_{n-3}(2,1) = 5p + 30, \quad n \geq 7.$

iii) $\Psi^p_{n-3}(3) = \begin{cases} 6, & n = 7 \\ 8, & n = 8 \\ 9, & n \geq 9 \end{cases}.$

From this lemma, equation (4·1) immediately gives us the following formulas for the number of groups of order p^n and coexponent 3 where $p \geq 5$ and $n \geq 7$.

Theorem 5·2. *For a prime $p \geq 5$ and a natural number n greater than or equal to 7, the number $\Psi^p_{3,n}$ of groups of order p^n and coexponent 3 is given by*

i) $\Psi^p_{3,n} = 5p + 2(p-1,3) + (p-1,4) + 59, \quad n = 7.$

ii) $\Psi^p_{3,n} = 5p + 2(p-1,3) + (p-1,4) + 61, \quad n = 8.$

iii) $\Psi^p_{3,n} = 5p + 2(p-1,3) + (p-1,4) + 62, \quad n \geq 9.$ □

The problem of determining the p-groups of coexponent 3 has been attempted before and for odd primes p a solution was claimed in the paper [23] :

L. I. Neikirk, Groups of order p^m, which contain cyclic subgroups of order p^{m-3}, Trans. Am. Math. Soc. **6** 316–325, (1905).

The formulas we give in part iii) of lemma 5·1 agrees with the formula given in [23], but the formulas corresponding to parts i) and ii) of lemma 5·1 differ from ours in that he claims that for $p \geq 5$ and $n \geq 7$

$$\Psi^p_{n-3}(2,1) = 5p + 32 \quad \text{and} \quad \Psi^p_{n-3}(1,1,1) = 23.$$

The approach Neikirk takes to this problem is via generators and relations, analogous to that used by Burnside in [3] on his work on p-groups of coexponent 2. In this book, Burnside warns that the final step in any classification by this method is to check that the groups have the correct order. This step has not been performed in Neikirk's calculations since the first group in his summary table for the groups corresponding to the formula $\Psi^p_{n-3}(2,1)$ is given as

$$G = \langle u, v, w \mid u^{p^{n-3}} = v^{p^3} = w^p = 1\,,\ (u,v) = u^{p^{n-3}},\ (u,w) = u^{p^{n-4}},\ (v,w) = v^p \rangle$$

and in this group we see that u generates a normal cyclic subgroup N which must have order at most p^{n-4} so that the automorphism induced on N by v has order p (this is the case since $(v,w) = v^p$ and $\mathrm{Aut}(N)$ is Abelian). We can therefore replace the relation $u^{p^{n-3}} = 1$ by the relation $u^{p^{n-4}} = 1$, and then it is straightforward to see that G is a split extension of the cyclic group of order p^{n-4} by the non-Abelian group of order p^3 and exponent p^2. But then G has order p^{n-1} and not p^n as claimed.

The work for lemma 5·1 was done before we discovered Neikirk's paper [23] and is therefore independent. Previously we had found the paper [29] by Titov from 1980 with a rather misleading title

"Groups containing a cyclic subgroup of index p^3", Mat. Zametki **28**, no. 1, 17–24, 167 (1980),

in which he determines certain quotients of p-groups of coexponent 3. In this paper, Titov states that the general determination problem is still to be considered.

To derive the formulas given in lemma 5·1 we use the Lie ring techniques of the previous chapter and we present full calculations for part ii) of lemma 5·1 in section 5·2. The three cases in part iii) of lemma 5·1 are all similar (and straightforward) and in section 5·3 we include the calculations for $\Psi^p_{n-3}(3)$ for $n = 7$, and give a summary of the Lie rings which arise in the cases $n = 8$ and $n \geq 9$. The proof of part i) of lemma 5·1 is as follows.

Proof of lemma 5·1. i)
For $p \geq 5$ and $n \geq 5$ we know from theorem 4·10 that $\Psi^p_{n-3}(1,1,1) = \Psi^p_2(1,1,1)$ which equals the number of groups of order p^5 of *type* $(2,1,1,1)$. The most recent published list of groups of order p^5 that we know of is given in [12] and these are tabulated by their type invariants. From this list we can see that for $p \geq 5$ the number of regular p-groups of *type* $(2,1,1,1)$ is given by $23 + 2(p-1,3) + (p-1,4)$. □

Remark. As mentioned before, the formula we give therefore depends on the classification of groups of order p^5 being correct for $p \geq 5$. These groups have been the subject of a number of papers, among them [1], [26] and [12], and they all agree on the correct number in the case $p \geq 5$. This formula was also reiterated as being correct in the recent paper [24] by Newman. The dependence on the residue class modulo 12 is a contribution from the groups of maximal nilpotency class 4, and this is in accordance with Blackburn's results in [2].

Section 5·2. The Calculation of $\Psi^p_{n-3}(2,1)$ for $p \geq 5$ and $n \geq 7$.

Throughout this section (and its subsections) p will denote a fixed arbitrary prime greater than 3, and n will denote a fixed arbitrary natural number greater than 6. We will also freely use the notation developed in chapter 4 and the reader is referred to that chapter for the relevant definitions.

Since we are assuming that p is greater than 3 it follows from theorem 4·10 that $\Psi^p_{n-3}(2,1)$ equals the number of isomorphism classes $\Delta^p_{n-3}(2,1)$ of nilpotent Lie rings in $\mathcal{F}^p_{n-3}(2,1)$, and by equation (4·9) we know that

$$\Delta^p_{n-3}(2,1) \quad = \sum_{U \in \mathcal{N}^p(2,1)} \Delta^p_{n-3}(2,1,U)\,, \tag{5·1}$$

where $\mathcal{N}^p(2,1)$ is a transversal for the isomorphism classes of nilpotent Lie rings satisfying the properties given in (4·4) (with $\lambda_1 = 2$, $\lambda_2 = 1$ and $t = 2$). Our plan of attack is therefore to calculate an appropriate transversal $\mathcal{N}^p(2,1)$ (which turns out to have 3 elements),

and then for each of the Lie rings U in $\mathcal{N}^p(2,1)$, calculate $\Delta^p_{n-3}(2,1,U)$ by using lemma 4·5 (having first computed the appropriate derivations and automorphisms of U).

Section 5·2·1. A Transversal $\mathcal{N}^p(2,1)$.

Recall that $\mathcal{N}^p(2,1)$ is a transversal for the nilpotent Lie rings U of order p^5 and *type* $(2,2,1)$ which possess a basis (z,u_1,u_2) corresponding to the type invariants where $z \in Z(U)$. It therefore suffices to determine the isomorphism classes of nilpotent Lie rings whose underlying Abelian group is

$$A = \left(\mathbb{Z}/p^2\mathbb{Z}\right) z \ \oplus \ \left(\mathbb{Z}/p^2\mathbb{Z}\right) u_1 \ \oplus \ \left(\mathbb{Z}/p\mathbb{Z}\right) u_2 \tag{5·2}$$

where $[z,z] = [z,u_1] = [u_1,z] = [z,u_2] = [u_2,z] = 0$. Now a Lie ring bracket on any finitely generated Abelian group is uniquely determined by its restriction to pairs of basis elements (since it is biadditive), and since in the situation here the Lie ring axioms also imply that we must have $[u_1,u_1] = [u_2,u_2] = 0$ and $[u_1,u_2] = -[u_2,u_1]$, it follows that any Lie ring bracket on A with z central is uniquely determined by the value of $[u_1,u_2]$. Now since u_2 has order p we must also have $[u_1,u_2] \in \Omega_1(A)$, and it is clear that this condition (together with the other conditions) is sufficient to guarantee a (unique) extension to a ring (i.e. $\mathbb{Z}-$algebra) structure on A satisfying $[x,x] = 0$ for any $x \in A$. It is then straightforward to see that the Jacobi identity holds in such a ring, and so the Lie ring structures on A with z central are given by

$$[u_1,u_2] = \alpha_1 pz + \alpha_2 pu_1 + \alpha_3 u_2 \quad \text{where } \alpha_1,\alpha_2,\alpha_3 \in \mathbb{Z}\,,$$

and such a Lie ring is nilpotent if and only if $\alpha_3 \equiv 0 \pmod p$. Now if $[u_1,u_2] \neq 0$ then the resulting Lie ring L is non-Abelian and either $\alpha_1 \not\equiv 0 \pmod p$ or $\alpha_2 \not\equiv 0 \pmod p$. If $\alpha_2 \not\equiv 0 \pmod p$ then letting V be the Lie ring on A with $[u_1,u_2]_V = pu_1$, we see that $V \cong L$ by the isomorphism $\theta : V \to L$ given by

$$z\theta = z\,, \quad u_1\theta = \alpha_1 z + \alpha_2 u_1\,, \quad u_2\theta = \alpha_2^{-1} u_2.$$

Otherwise we must have $\alpha_2 \equiv 0 \pmod p$ and $\alpha_1 \not\equiv 0 \pmod p$, and then letting W be the Lie ring on A with $[u_1,u_2]_W = pz$ we see that $W \cong L$ by the isomorphism $\psi : W \to L$

given by

$$z\psi = z\,, \quad u_1\psi = u_1\,, \quad u_2\psi = \alpha_1^{-1}u_2.$$

Now it is easy to see that

$$Z(V) = \langle z\rangle \oplus \langle pu_1\rangle\,, \quad [V,V] = \langle pu_1\rangle\,, \quad Z(W) = \langle z\rangle \oplus \langle pu_1\rangle\,, \quad [W,W] = \langle pz\rangle\,,$$

from which it follows that

$$[W,W] \cap \mathfrak{U}_1(Z(W)) \neq \{0\} \qquad \text{and} \qquad [V,V] \cap \mathfrak{U}_1(Z(V)) = \{0\}\,,$$

so that $W \ncong V$. So letting X be the Abelian Lie ring on A we see that we can take

$$\mathcal{N}^p(2,1) = \{V, W, X\}.$$

We now summarise the approach we will use to calculate $\Delta_k^p(2,1,U)$ where $k = n-3 \geq 4$ and $U \in \mathcal{N}^p(2,1)$. Recall (from chapter 4) that $\Delta_k^p(2,1,U)$ is the number of isomorphism classes of nilpotent Lie rings L in $\mathcal{F}_k^p(2,1)$ with $\Omega_2(L) \cong U$, and from part i) of theorem 4·6 we know that such a Lie ring is isomorphic to (at least) one of the Lie rings

$$\bigcup_{\substack{c \in U \\ \text{central of order } p^2}} \{\, U^{\sigma}_{c,e_k} \;:\; \sigma \text{ a nilpotent element of } \mathrm{Der}(U)_c \,\}.$$

Moreover, for any nilpotent elements $\sigma \in \mathrm{Der}(U)_z$ and $\tau \in \mathrm{Der}(U)_{z'}$, lemma 4·5 (i) and (ii) gave the necessary and sufficient conditions for U^{σ}_{z,e_k} to be isomorphic to U^{τ}_{z',e_k}. Each choice of $U \in \{V,\ W,\ X\}$ was constructed above with a distinguished central element of order p^{λ_1}, which we labelled z. As long as U is one of these three Lie rings, it is easy to see that for any other central element z' of U of order p^2, there is an automorphism $\pi \in \mathrm{Aut}_{\mathrm{Lie}}(U)$ such that $z' = z\pi$. Conditions (i) and (ii) of lemma 4·5 (with $\alpha = 1$ and $x = 0$) show that for any derivation $\tau \in \mathrm{Der}(U)_{z'}$ the Lie ring U^{τ}_{z',e_k} is isomorphic to the Lie ring U^{σ}_{z,e_k}, with the derivation $\sigma \in \mathrm{Der}(U)_z$ defined by the rule $\sigma = \pi\tau\pi^{-1}$. Because of this, every isomorphism type is already represented by a Lie ring of the form U^{σ}_{z,e_k} for this one choice of z, **which we assume fixed from now on**. The following conditions ((i) and (ii) of lemma 4·5 with $z = z'$)

$$\begin{aligned} &\text{i)} \quad z\pi = \alpha z \text{ for some } \alpha \in \mathbb{Z} \text{ with } (\alpha, p) = 1. \\ &\text{ii)} \quad \sigma\pi = \pi(\mathrm{ad}_r x + \alpha\tau) \text{ for some } x \in U. \end{aligned} \tag{5·3}$$

therefore define an equivalence relation $\sim$ on $\mathrm{Der}(U)_z$ such that $\Delta_k^p(2,1,U)$ equals the number of $\sim$–classes of nilpotent elements in $\mathrm{Der}(U)_z$ (observe that since nilpotency is an isomorphism invariant, it is also a $\sim$–invariant). Now relative to the fixed basis (z, u_1, u_2) of A, $\mathrm{Hom}_{\mathbb{Z}}(A, A)$ is isomorphic to the ring of matrices of the form

$$\begin{pmatrix} \mathbb{Z}/p^2\mathbb{Z} & \mathbb{Z}/p^2\mathbb{Z} & \mathbb{Z}/p\mathbb{Z} \\ \mathbb{Z}/p^2\mathbb{Z} & \mathbb{Z}/p^2\mathbb{Z} & \mathbb{Z}/p\mathbb{Z} \\ p\mathbb{Z}/p^2\mathbb{Z} & p\mathbb{Z}/p^2\mathbb{Z} & \mathbb{Z}/p\mathbb{Z} \end{pmatrix} \tag{5·4}$$

and with this identification, the ***nilpotent*** elements of $\mathrm{Der}(U)_z$ correspond to certain matrices of the form

$$\begin{pmatrix} 0 & 0 & 0 \\ \mathbb{Z}/p^2\mathbb{Z} & p\mathbb{Z}/p^2\mathbb{Z} & \mathbb{Z}/p\mathbb{Z} \\ p\mathbb{Z}/p^2\mathbb{Z} & p\mathbb{Z}/p^2\mathbb{Z} & 0 \end{pmatrix} \tag{5·5}$$

and the Lie ring automorphisms of U which fix $\langle z \rangle$ set–wise correspond to certain matrices of the form

$$\begin{pmatrix} \mathbb{Z}/p^2\mathbb{Z} & 0 & 0 \\ \mathbb{Z}/p^2\mathbb{Z} & \mathbb{Z}/p^2\mathbb{Z} & \mathbb{Z}/p\mathbb{Z} \\ p\mathbb{Z}/p^2\mathbb{Z} & p\mathbb{Z}/p^2\mathbb{Z} & \mathbb{Z}/p\mathbb{Z} \end{pmatrix} \tag{5·6}$$

with the diagonal entries coprime to p (so that the corresponding morphism of A belongs to $\mathrm{Aut}_{\mathbb{Z}}(A)$). Once we have determined which matrices of the form (5·5) give derivations, and which matrices of the form (5·6) preserve the Lie bracket on U, the relation $\sim$ can be replaced by a set of congruences in the corresponding matrix entries where the indeterminates are the entries of the automorphism matrix and the inner derivation matrix corresponding to the automorphism and inner derivation in condition ii) of (5·3). Solving these congruences will then enable us to determine the matrices corresponding to a set of representatives for the $\sim$–classes. We deal with each element of $\mathcal{N}^p(2,1)$ separately in the following subsections where the basis of A will always be fixed as (z, u_1, u_2) so that we can unambiguously identify $\mathrm{Hom}_{\mathbb{Z}}(A, A)$ with the ring of matrices (5·4).

Section 5·2·2. Calculation of Δ^p_{n-3} (2,1,V) .

Recall that V is the Lie ring on A where z is central and $[u_1, u_2] = pu_1$. We first determine which matrices of the form (5·5) are derivations of V, so let

$$\kappa = \begin{pmatrix} 0 & 0 & 0 \\ a_1 & pa_2 & a_3 \\ pb_1 & pb_2 & 0 \end{pmatrix}$$

be such a matrix. In order that κ be a derivation we must have

$$[u_1, u_2]\kappa = [u_1\kappa, u_2] + [u_1, u_2\kappa]$$

and it is straightforward to see that this condition is sufficient also. Hence $\kappa \in \mathrm{Der}(V)_z$ if and only if $pa_1 z = 0$ which is equivalent to requiring that $a_1 \equiv 0 \pmod{p}$. So the nilpotent elements of $\mathrm{Der}(V)_z$ are the matrices of the form

$$\begin{pmatrix} 0 & 0 & 0 \\ p\mathbb{Z}/p^2\mathbb{Z} & p\mathbb{Z}/p^2\mathbb{Z} & \mathbb{Z}/p\mathbb{Z} \\ p\mathbb{Z}/p^2\mathbb{Z} & p\mathbb{Z}/p^2\mathbb{Z} & 0 \end{pmatrix}, \tag{5·7}$$

and it is straightforward to see that the inner derivations of V are the matrices of the form

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & p\mathbb{Z}/p^2\mathbb{Z} & 0 \\ 0 & p\mathbb{Z}/p^2\mathbb{Z} & 0 \end{pmatrix}. \tag{5·8}$$

Now if $\sigma \in \mathrm{Der}(V)_z$ and $x \in V$ then from condition ii) of (5·3) it follows that $\sigma \sim \sigma + \mathrm{ad}_r x$, and so since we are only interested in the $\sim$–classes, we can restrict attention to the nilpotent elements of $\mathrm{Der}(V)_z$ of the form

$$\begin{pmatrix} 0 & 0 & 0 \\ p\mathbb{Z}/p^2\mathbb{Z} & 0 & \mathbb{Z}/p\mathbb{Z} \\ p\mathbb{Z}/p^2\mathbb{Z} & 0 & 0 \end{pmatrix}. \tag{5·9}$$

We now determine which matrices of the form (5·6) are automorphisms of V, so let

$$\pi = \begin{pmatrix} \alpha & 0 & 0 \\ \beta_1 & \beta_2 & \beta_3 \\ p\gamma_1 & p\gamma_2 & \gamma_3 \end{pmatrix}$$

be such a matrix and observe that $\pi \in \mathrm{Aut}_{\mathbf{Z}}(A)$ if and only if $(\alpha, p) = (\beta_2, p) = (\gamma_3, p) = 1$. Since $\langle z \rangle \pi = \langle z \rangle$, it is straightforward to see that the condition that $\pi \in \mathrm{Aut}_{\mathrm{Lie}}(V)$ is given by

$$[u_1, u_2]\pi = [u_1\pi, u_2\pi]$$

and so $\pi \in \mathrm{Aut}_{\mathrm{Lie}}(V)$ if and only if $p\beta_1 z + p\beta_2 u_1 = p\beta_2\gamma_3 u_1$, which is equivalent to requiring that $\beta_1 \equiv 0 \pmod{p}$ and $\gamma_3 \equiv 1 \pmod{p}$. Therefore the automorphisms of V fixing $\langle z \rangle$ set-wise are of the form

$$\begin{pmatrix} \alpha & 0 & 0 \\ p\beta_1 & \beta_2 & \beta_3 \\ p\gamma_1 & p\gamma_2 & 1 \end{pmatrix} \qquad \text{with} \quad (\alpha, p) = (\beta_2, p) = 1. \tag{5·10}$$

We now determine the system of congruences for $\sim$–equivalence between two derivations σ, τ of the form (5·9), so let

$$\sigma = \begin{pmatrix} 0 & 0 & 0 \\ pa_1 & 0 & a_3 \\ pb_1 & 0 & 0 \end{pmatrix} \qquad \text{and} \qquad \tau = \begin{pmatrix} 0 & 0 & 0 \\ pc_1 & 0 & c_3 \\ pd_1 & 0 & 0 \end{pmatrix}.$$

Then by conditions i) and ii) of (5·3), $\sigma \sim \tau$ if and only if there exist matrices

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & p\lambda_1 & 0 \\ 0 & p\lambda_2 & 0 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} \alpha & 0 & 0 \\ p\beta_1 & \beta_2 & \beta_3 \\ p\gamma_1 & p\gamma_2 & 1 \end{pmatrix} \qquad \text{with} \quad (\alpha, p) = (\beta_2, p) = 1$$

such that

$$\begin{pmatrix} 0 & 0 & 0 \\ pa_1 & 0 & a_3 \\ pb_1 & 0 & 0 \end{pmatrix} \begin{pmatrix} \alpha & 0 & 0 \\ p\beta_1 & \beta_2 & \beta_3 \\ p\gamma_1 & p\gamma_2 & 1 \end{pmatrix} = \begin{pmatrix} \alpha & 0 & 0 \\ p\beta_1 & \beta_2 & \beta_3 \\ p\gamma_1 & p\gamma_2 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ p\alpha c_1 & p\lambda_1 & \alpha c_3 \\ p\alpha d_1 & p\lambda_2 & 0 \end{pmatrix}$$

(where equality here is in the ring given in (5·4)). This gives the following system of congruences

$$\begin{aligned}
\alpha\,,\,\beta_2 &\not\equiv 0 && \pmod{p} \\
p(a_1\alpha + a_3\gamma_1) &\equiv p\alpha(\beta_2 c_1 + \beta_3 d_1) && \pmod{p^2} \\
pa_3\gamma_2 &\equiv p(\beta_2\lambda_1 + \beta_3\lambda_2) && \pmod{p^2} \\
a_3 &\equiv \beta_2\alpha c_3 && \pmod{p} \\
pb_1\alpha &\equiv p\alpha d_1 && \pmod{p^2} \\
p\lambda_2 &\equiv 0 && \pmod{p^2}
\end{aligned}$$

which reduces to the system

$$\left.\begin{array}{rcll} \alpha\,,\beta_2 & \not\equiv & 0 & (\mathrm{mod}\ p) \\ a_1\alpha + a_3\gamma_1 & \equiv & \beta_2\alpha c_1 + \beta_3\alpha d_1 & (\mathrm{mod}\ p) \\ a_3\gamma_2 & \equiv & \beta_2\lambda_1 & (\mathrm{mod}\ p) \\ a_3 & \equiv & \beta_2\alpha c_3 & (\mathrm{mod}\ p) \\ b_1 & \equiv & d_1 & (\mathrm{mod}\ p) \end{array}\right\} \qquad (5{\cdot}11)$$

The third equation in this system can be ignored since λ_1 can always be chosen to solve this equation given solutions to the others. Observe that the fourth equation implies that we must have $a_3 \equiv c_3 \equiv 0 \pmod{p}$ or $a_3, c_3 \not\equiv 0 \pmod{p}$ in order that $\sigma \sim \tau$, and so this gives the following two mutually exclusive cases.

Case 1. $a_3 \equiv c_3 \equiv 0 \pmod{p}$.

If $b_1 \equiv d_1 \equiv 0 \pmod{p}$ then the system (5·11) can be solved if and only if $a_1 \equiv c_1 \equiv 0 \pmod{p}$ or $a_1, c_1 \not\equiv 0 \pmod{p}$. If $b_1 \equiv d_1 \not\equiv 0 \pmod{p}$ then the system can always be solved. We therefore have $p+1$ distinct $\sim$-classes in case 1 with the following representatives

$$\begin{pmatrix} 0 & 0 & 0 \\ p & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ p\epsilon & 0 & 0 \end{pmatrix} \quad 0 \le \epsilon \le p-1. \qquad (5{\cdot}12)$$

Case 2. $a_3 \equiv c_3 \not\equiv 0 \pmod{p}$.

In this case the system is always soluble and so we have p distinct $\sim$-classes with the representatives

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ p\epsilon & 0 & 0 \end{pmatrix} \quad 0 \le \epsilon \le p-1. \qquad (5{\cdot}13)$$

We have therefore shown that $\Delta^p_{n-3}(2,1) = 2p+1$ and representatives for the $\sim$-classes are given by (5·12) and (5·13).

Section 5·2·3. Calculation of Δ^p_{n-3} (2,1,W) .

Recall that W is the Lie ring on A with z central and $[u_1, u_2] = pz$. The method of calculation is entirely analogous to the previous section and so we first determine which matrices of the form (5·5) are derivations of W. If κ is such a matrix then it is easy to see that in this situation we automatically have $[u_1, u_2]\kappa = [u_1\kappa, u_2] + [u_1, u_2\kappa]$, and so any matrix of the form (5·5) is a nilpotent element of $\mathrm{Der}(W)_z$. The inner derivations of W are seen to be the matrices of the form

$$\begin{pmatrix} 0 & 0 & 0 \\ p\mathbb{Z}/p^2\mathbb{Z} & 0 & 0 \\ p\mathbb{Z}/p^2\mathbb{Z} & 0 & 0 \end{pmatrix} \tag{5·14}$$

and so any nilpotent element of $\mathrm{Der}(W)_z$ is $\sim$-equivalent to a derivation of the form

$$\begin{pmatrix} 0 & 0 & 0 \\ \mathbb{Z}/p\mathbb{Z} & p\mathbb{Z}/p^2\mathbb{Z} & \mathbb{Z}/p\mathbb{Z} \\ 0 & p\mathbb{Z}/p^2\mathbb{Z} & 0 \end{pmatrix} \tag{5·15}$$

and so we can restrict attention to derivations of this form.

If we now let

$$\pi = \begin{pmatrix} \alpha & 0 & 0 \\ \beta_1 & \beta_2 & \beta_3 \\ p\gamma_1 & p\gamma_2 & \gamma_3 \end{pmatrix}$$

be a matrix of the form (5·6) with $(\alpha, p) = (\beta_2, p) = (\gamma_3, p) = 1$, then the condition that $\pi \in \mathrm{Aut}_{\mathrm{Lie}}(W)$ is given by

$$\alpha pz = \beta_2\gamma_3 pz$$

and this is equivalent to requiring that $\alpha \equiv \beta_2\gamma_3 \pmod{p}$. Therefore the automorphisms of W fixing $\langle z \rangle$ set-wise are the matrices of the form

$$\begin{pmatrix} \alpha & 0 & 0 \\ \beta_1 & \beta_2 & \beta_3 \\ p\gamma_1 & p\gamma_2 & \gamma_3 \end{pmatrix} \quad \text{with} \quad \begin{array}{rcll} \alpha\,,\,\beta_2\,,\,\gamma_3 & \not\equiv & 0 & \pmod{p} \\ \alpha & \equiv & \beta_2\gamma_3 & \pmod{p} \end{array} \tag{5·16}$$

If we now let

$$\sigma = \begin{pmatrix} 0 & 0 & 0 \\ a_1 & pa_2 & a_3 \\ 0 & pb_2 & 0 \end{pmatrix} \quad \text{and} \quad \tau = \begin{pmatrix} 0 & 0 & 0 \\ c_1 & pc_2 & c_3 \\ 0 & pd_2 & 0 \end{pmatrix}$$

be derivations of the form (5·15), then $\sigma \sim \tau$ if and only if there exist matrices

$$\begin{pmatrix} 0 & 0 & 0 \\ p\lambda_1 & 0 & 0 \\ p\lambda_2 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \alpha & 0 & 0 \\ \beta_1 & \beta_2 & \beta_3 \\ p\gamma_1 & p\gamma_2 & \gamma_3 \end{pmatrix} \quad \text{with} \quad \begin{array}{rcll} \alpha\,,\,\beta_2\,,\,\gamma_3 & \not\equiv & 0 & (\mathrm{mod}\ p) \\ \alpha & \equiv & \beta_2\gamma_3 & (\mathrm{mod}\ p) \end{array}$$

such that

$$\begin{pmatrix} 0 & 0 & 0 \\ a_1 & pa_2 & a_3 \\ 0 & pb_2 & 0 \end{pmatrix} \begin{pmatrix} \alpha & 0 & 0 \\ \beta_1 & \beta_2 & \beta_3 \\ p\gamma_1 & p\gamma_2 & \gamma_3 \end{pmatrix} = \begin{pmatrix} \alpha & 0 & 0 \\ \beta_1 & \beta_2 & \beta_3 \\ p\gamma_1 & p\gamma_2 & \gamma_3 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ \alpha c_1 + p\lambda_1 & p\alpha c_2 & \alpha c_3 \\ p\lambda_2 & p\alpha d_2 & 0 \end{pmatrix}.$$

This matrix equation then gives the following system of congruences (split into two parts)

$$\left.\begin{array}{rcll} \alpha\,,\,\beta_2\,,\,\gamma_3 & \not\equiv & 0 & (\mathrm{mod}\ p) \\ \alpha & \equiv & \beta_2\gamma_3 & (\mathrm{mod}\ p) \end{array}\right\} \tag{5·17}$$

$$\left.\begin{array}{rcll} a_1\alpha + p(a_2\beta_1 + a_3\gamma_1) & \equiv & \beta_2\alpha c_1 + p(\beta_2\lambda_1 + \beta_3\lambda_2) & (\mathrm{mod}\ p^2) \\ p(a_2\beta_2 + a_3\gamma_2) & \equiv & p\alpha(\beta_2 c_2 + \beta_3 d_2) & (\mathrm{mod}\ p^2) \\ a_3\gamma_3 & \equiv & \beta_2\alpha c_3 & (\mathrm{mod}\ p) \\ pb_2\beta_1 & \equiv & p(\gamma_2\alpha c_1 + \gamma_3\lambda_2) & (\mathrm{mod}\ p^2) \\ pb_2\beta_2 & \equiv & p\alpha d_2\gamma_3 & (\mathrm{mod}\ p^2) \end{array}\right\} \tag{5·18}$$

The first equation of (5·18) implies that we must have $a_1\alpha \equiv \beta_2\alpha c_1 \pmod{p}$, and this together with the first two equations imply that we must have $a_1 \equiv c_1 \equiv 0 \pmod{p}$ or $a_1, c_1 \not\equiv 0 \pmod{p}$ in order that the system (5·17) and (5·18) has a solution. We therefore have two mutually exclusive cases.

Case 1. $a_1 \equiv c_1 \equiv 0 \pmod{p}$.

Choosing integers a_1' and c_1' so that $pa_1' \equiv a_1 \pmod{p^2}$ and $pc_1' \equiv c_1 \pmod{p^2}$, we see that in this case, $\sigma \sim \tau$ if and only if the system consisting of (5·17) together with

$$\left.\begin{array}{rcll} a_1'\alpha + a_2\beta_1 + a_3\gamma_1 & \equiv & \beta_2\alpha c_1' + \beta_2\lambda_1 + \beta_3\lambda_2 & (\mathrm{mod}\ p) \\ a_2\beta_2 + a_3\gamma_2 & \equiv & \alpha\beta_2 c_2 + \beta_3 d_2 & (\mathrm{mod}\ p) \\ a_3\gamma_3 & \equiv & \beta_2\alpha c_3 & (\mathrm{mod}\ p) \\ b_2\beta_1 & \equiv & \gamma_3\lambda_2 & (\mathrm{mod}\ p) \\ b_2\beta_2 & \equiv & \alpha d_2\gamma_3 & (\mathrm{mod}\ p) \end{array}\right\} \tag{5·19}$$

has a solution.

Now the first and fourth equations of (5·19) can be ignored since λ_1 and λ_2 can be chosen to solve these once a solution to the other equations is found (using the fact that γ_3 and β_2 must be coprime to p), so the system reduces to (5·17) together with

$$\left.\begin{array}{rcll} a_2\beta_2 + a_3\gamma_2 & \equiv & \alpha\beta_2 c_2 + \beta_3 d_2 & (\mathrm{mod}\ p) \\ a_3\gamma_3 & \equiv & \beta_2\alpha c_3 & (\mathrm{mod}\ p) \\ b_2\beta_2 & \equiv & \alpha d_2\gamma_3 & (\mathrm{mod}\ p) \end{array}\right\} \qquad (5\cdot20)$$

Now by the first equation of (5·17) we must have $\alpha, \beta_2, \gamma_3$ coprime to p and so the second and third equations of (5·20) give us the following four mutually exclusive subcases.

Case 1.1. $a_3 \equiv c_3 \equiv 0 \pmod{p}$ and $b_2 \equiv d_2 \equiv 0 \pmod{p}$.

In this case, (5·20) reduces to the single equation $a_2 \equiv \alpha c_2 \pmod{p}$, and this together with (5·17) has a solution if and only if $a_2 \equiv c_2 \equiv 0 \pmod{p}$ or $a_2, c_2 \not\equiv 0 \pmod{p}$. We therefore have two distinct $\sim$–classes in this subcase with representatives

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Case 1.2. $a_3 \equiv c_3 \equiv 0 \pmod{p}$ and $b_2, d_2 \not\equiv 0 \pmod{p}$.

In this case we can use the first equation of (5·17) to substitute for α in the third equation of (5·20) so that (5·20) becomes

$$\begin{array}{rcll} a_2\beta_2 & \equiv & \alpha\beta_2 c_2 + \beta_3 d_2 & (\mathrm{mod}\ p) \\ b_2 & \equiv & d_2\gamma_3^2 & (\mathrm{mod}\ p) \end{array}$$

It therefore follows that a necessary condition for $\sigma \sim \tau$ in this case is for b_2 and d_2 to have the same quadratic character modulo p, and given that this condition holds, it is straightforward to see that this system together with (5·17) can be solved. So if we let $\nu \in \mathbb{Z}$ be a be a fixed non-quadratic residue modulo p then we have two distinct $\sim$–classes in this subcase with representatives

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & p & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & p\nu & 0 \end{pmatrix}.$$

Case 1.3. $a_3, c_3 \not\equiv 0 \pmod{p}$ and $b_2 \equiv d_2 \equiv 0 \pmod{p}$.

In this case we can use the first equation of (5·17) to substitute for α in the second equation of (5·20), so that (5·20) becomes

$$\begin{aligned} a_2\beta_2 + a_3\gamma_2 &\equiv \alpha\beta_2 c_2 \pmod{p} \\ a_3 &\equiv c_3\beta_2^2 \pmod{p} \end{aligned}$$

We then see that a necessary condition for $\sigma \sim \tau$ in this case is for a_3 and c_3 to have the same quadratic character modulo p, and this is also a sufficient condition. Hence if ν denotes a fixed non-quadratic residue modulo p, we have two distinct $\sim$–classes in this subcase with representatives

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & \nu \\ 0 & 0 & 0 \end{pmatrix}.$$

Case 1.4. $a_3, c_3 \not\equiv 0 \pmod{p}$ and $b_2, d_2 \not\equiv 0 \pmod{p}$.

In this case we use the first equation of (5·17) to eliminate α from the second and third equations of (5·20) which then becomes

$$\begin{aligned} a_2\beta_2 + a_3\gamma_2 &\equiv \alpha\beta_2 c_2 + \beta_3 d_2 \pmod{p} \\ a_3 &\equiv c_3\beta_2^2 \pmod{p} \\ b_2 &\equiv d_2\gamma_3^2 \pmod{p} \end{aligned}$$

We therefore see that necessary conditions for $\sigma \sim \tau$ in this case are that a_3 and d_3 have the same quadratic character modulo p, and b_2 and d_2 have the same quadratic character modulo p. If these conditions hold then it is easy to see that this system together with (5·17) has a solution. Hence there are four distinct $\sim$–classes in this subcase with the following representatives (again, ν denotes a fixed non-quadratic residue modulo p)

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & p & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & \nu \\ 0 & p & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & p\nu & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & \nu \\ 0 & p\nu & 0 \end{pmatrix}.$$

So summarising, in case 1 we have 10 distinct $\sim$–classes. We now deal with case 2.

Case 2. $a_1, c_1 \not\equiv 0 \pmod{p}$.

In this case the first equation of (5·18) implies that we must have $\beta_2 \equiv a_1 c_1^{-1} \pmod{p}$ for the system (5·17) and (5·18) to have a solution. Now if we have a solution to the system consisting of (5·17) together with the second, third and fifth equations of (5·18) (i.e. the equations not involving λ_1 and λ_2) together with this constraint on β_2, then λ_2 can be chosen to solve the fourth equation of (5·18) (since γ_3 must be coprime to p) and then choosing $\lambda_1 \equiv 0 \pmod{p}$ we can lift β_2 to give a solution to the first equation of (5·17) (since αc_1 is coprime to p). Therefore in this case we can ignore the first and fourth equations of (5·18) provided we keep the constraint on β_2, and so in this case the system we consider is

$$\left.\begin{aligned} \alpha, \gamma_3 &\not\equiv 0 \pmod{p} \\ \alpha &\equiv \beta_2\gamma_3 \pmod{p} \\ \beta_2 &\equiv a_1 c_1^{-1} \pmod{p} \end{aligned}\right\} \tag{5·21}$$

$$\left.\begin{aligned} a_2\beta_2 + a_3\gamma_2 &\equiv c_2\alpha\beta_2 + d_2\alpha\beta_3 \pmod{p} \\ a_3\gamma_3 &\equiv c_3\alpha\beta_2 \pmod{p} \\ b_2\beta_2 &\equiv d_2\alpha\gamma_3 \pmod{p} \end{aligned}\right\} \tag{5·22}$$

Now since we must have $\alpha, \beta_2, \gamma_3$ coprime to p, the second and third equations in (5·22) imply that we have the following four mutually exclusive subcases.

Case 2.1. $a_3 \equiv c_3 \equiv 0 \pmod{p}$ and $b_2 \equiv d_2 \equiv 0 \pmod{p}$.

In this case the first equation of (5·22) implies that $\sigma \sim \tau$ only if $a_2 \equiv c_2 \equiv 0 \pmod{p}$ or $a_2, c_2 \not\equiv 0 \pmod{p}$, and either of these is easily seen to be sufficient as well, so that in this subcase we have two distinct $\sim$–classes with representatives

$$\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 0 & 0 \\ 1 & p & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Case 2.2. $a_3 \equiv c_3 \equiv 0 \pmod{p}$ and $b_2, d_2 \not\equiv 0 \pmod{p}$.

In this case (5·22) reduces to the following (using the second equation of (5·21) to substitute for α in the third equation of (5·22))

$$\begin{aligned} a_2\beta_2 &\equiv c_2\alpha\beta_2 + d_2\alpha\beta_3 \pmod{p} \\ b_2 &\equiv d_2\gamma_3^2 \pmod{p} \end{aligned}$$

and so a necessary condition for $\sigma \sim \tau$ is that b_2 and d_2 have the same quadratic character modulo p. If this is the case then it is straightforward to see that the system (5·21) and (5·22) have a solution and so we have two distinct $\sim$–classes with the following representatives for a fixed non-quadratic residue ν modulo p

$$\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & p & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & p\nu & 0 \end{pmatrix}.$$

Case 2.3. $a_3, c_3 \not\equiv 0 \pmod{p}$ and $b_2 \equiv d_2 \equiv 0 \pmod{p}$.

In this case if we use (5·21) to eliminate α and β_2 from the second equation of (5·22) then (5·22) reduces to

$$\begin{aligned} a_2\beta_2 + a_3\gamma_2 &\equiv c_2\alpha\beta_2 \pmod{p} \\ a_3c_3^{-1} &\equiv (a_1c_1^{-1})^2 \pmod{p} \end{aligned}$$

Now the first equation here together with (5·21) always has a solution and so in this subcase, the condition for $\sigma \sim \tau$ is given by the second congruence here. Now for each pair (a_1, a_3) in $\mathbf{Z}/p\mathbf{Z}^\times \times \mathbf{Z}/p\mathbf{Z}^\times$ there are $((p-1)/2) \times 2$ pairs (c_1, c_3) in $\mathbf{Z}/p\mathbf{Z}^\times \times \mathbf{Z}/p\mathbf{Z}^\times$ satisfying this congruence. Therefore there are $|\mathbf{Z}/p\mathbf{Z}^\times \times \mathbf{Z}/p\mathbf{Z}^\times|/(p-1) = p-1$ distinct $\sim$–classes in this subcase. If we let ν denote a fixed non-quadratic residue modulo p and let h denote a fixed primitive element modulo p (i.e. h modulo p generates $\mathbf{Z}/p\mathbf{Z}^\times$), then the following are a set of representatives for the $\sim$–classes

$$\begin{pmatrix} 0 & 0 & 0 \\ h^r & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 & 0 \\ h^r & 0 & \nu \\ 0 & 0 & 0 \end{pmatrix} \qquad \text{where } r = 1, \ldots, \frac{p-1}{2}.$$

Case 2.4. $a_3, c_3 \not\equiv 0 \pmod{p}$ and $b_2, d_2 \not\equiv 0 \pmod{p}$.

In this case we use (5·21) to eliminate α and β_2 from the second and third equations of (5·22) so that (5·22) becomes

$$\begin{aligned} a_2\beta_2 + a_3\gamma_2 &\equiv c_2\alpha\beta_2 + d_2\alpha\beta_3 \pmod{p} \\ a_3c_3^{-1} &\equiv (a_1c_1^{-1})^2 \pmod{p} \\ b_2 &\equiv d_2\gamma_3^2 \pmod{p} \end{aligned}$$

Now if the second and third equations here have a solution then a solution can be obtained for the whole system, and so we only need to consider these two equations. It therefore follows that in this subcase $\sigma \sim \tau$ if and only if the second congruence here holds and b_2 and d_2 have the same quadratic character modulo p. By a similar discussion to that used in case 2.3 we see that there are $2(p-1)$ $\sim$–classes in this subcase and with ν and h having the same meaning as in case 2.3 we have the following representatives

$$\begin{pmatrix} 0 & 0 & 0 \\ h^r & 0 & 1 \\ 0 & p & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 & 0 \\ h^r & 0 & \nu \\ 0 & p & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 & 0 \\ h^r & 0 & 1 \\ 0 & p\nu & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 & 0 \\ h^r & 0 & \nu \\ 0 & p\nu & 0 \end{pmatrix} \qquad r = 1, \ldots, \frac{p-1}{2}.$$

So summarising case 2, we see that there are $3(p-1)+4 = 3p+1$ distinct $\sim$–classes. Putting case 1 and case 2 together, we have therefore shown that $\Delta^p_{n-3}(2,1,W) = 3p+11$.

Section 5·2·4. Calculation of Δ^p_{n-3} (2,1,X) .

Recall that X is the Lie ring on A with z central and $[u_1, u_2] = 0$, i.e. X is the unique Abelian Lie ring on A. Now since all the Lie products in X are 0 it follows that the inner derivations of X are all 0 and the nilpotent elements of $\mathrm{Der}(X)_z$ are precisely all the matrices of the form (5·5). In addition, the automorphisms of X fixing $\langle z \rangle$ set–wise are precisely all the matrices of the form (5·6) with the condition that the diagonal entries are coprime to p. It therefore follows that if we let σ and τ be two nilpotent elements of $\mathrm{Der}(X)_z$ where

$$\sigma = \begin{pmatrix} 0 & 0 & 0 \\ a_1 & pa_2 & a_3 \\ pb_1 & pb_2 & 0 \end{pmatrix} \qquad \text{and} \qquad \tau = \begin{pmatrix} 0 & 0 & 0 \\ c_1 & pc_2 & c_3 \\ pd_1 & pd_2 & 0 \end{pmatrix},$$

then $\sigma \sim \tau$ if and only if there exists a matrix

$$\pi = \begin{pmatrix} \alpha & 0 & 0 \\ \beta_1 & \beta_2 & \beta_3 \\ p\gamma_1 & p\gamma_2 & \gamma_3 \end{pmatrix} \qquad \text{with} \quad (\alpha, p) = (\beta_2, p) = (\gamma_3, p) = 1$$

such that

$$\begin{pmatrix} 0 & 0 & 0 \\ a_1 & pa_2 & a_3 \\ pb_1 & pb_2 & 0 \end{pmatrix} \begin{pmatrix} \alpha & 0 & 0 \\ \beta_1 & \beta_2 & \beta_3 \\ p\gamma_1 & p\gamma_2 & \gamma_3 \end{pmatrix} = \begin{pmatrix} \alpha & 0 & 0 \\ \beta_1 & \beta_2 & \beta_3 \\ p\gamma_1 & p\gamma_2 & \gamma_3 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ \alpha c_1 & p\alpha c_2 & \alpha c_3 \\ p\alpha d_1 & p\alpha d_2 & 0 \end{pmatrix}.$$

This matrix equation is equivalent to the following system of congruences having a solution for the entries of the matrix π.

$$\alpha\,,\,\beta_2\,,\,\gamma_3 \not\equiv 0 \pmod{p} \tag{5·23}$$

$$\left.\begin{aligned} a_1\alpha + p(a_2\beta_1 + a_3\gamma_1) &\equiv \beta_2\alpha c_1 + p\beta_3\alpha d_1 \pmod{p^2} \\ p(a_2\beta_2 + a_3\gamma_2) &\equiv p(\alpha\beta_2 c_2 + \alpha\beta_3 d_2) \pmod{p^2} \\ a_3\gamma_3 &\equiv \beta_2\alpha c_3 \pmod{p} \\ p(b_1\alpha + b_2\beta_1) &\equiv p(\alpha\gamma_2 c_1 + \alpha\gamma_3 d_1) \pmod{p^2} \\ pb_2\beta_2 &\equiv pd_2\alpha\gamma_3 \pmod{p^2} \end{aligned}\right\} \tag{5·24}$$

Now (5·23) and the first equation of (5·24) imply that we must have $a_1 \equiv \beta_2 c_1 \pmod{p}$, and so since we also must have β_2 coprime to p this gives us two mutually exclusive cases corresponding to the conditions $a_1 \equiv c_1 \equiv 0 \pmod{p}$ and $a_1, c_1 \not\equiv 0 \pmod{p}$.

Case 1. $a_1 \equiv c_1 \equiv 0 \pmod{p}$.

Letting a_1' and c_1' be integers such that $a_1 \equiv pa_1' \pmod{p^2}$ and $c_1 \equiv pc_1' \pmod{p^2}$, we see (from (5·24)) that in this case, $\sigma \sim \tau$ if and only if the following system together with (5·23) can be solved

$$\left.\begin{aligned} a_1'\alpha + a_2\beta_1 + a_3\gamma_1 &\equiv c_1'\alpha\beta_2 + d_1\alpha\beta_3 \pmod{p} \\ a_2\beta_2 + a_3\gamma_2 &\equiv c_2\alpha\beta_2 + d_2\alpha\beta_3 \pmod{p} \\ a_3\gamma_3 &\equiv c_3\alpha\beta_2 \pmod{p} \\ b_1\alpha + b_2\beta_1 &\equiv d_1\alpha\gamma_3 \pmod{p} \\ b_2\beta_2 &\equiv d_2\alpha\gamma_3 \pmod{p} \end{aligned}\right\} \tag{5·25}$$

The third and fifth equations together with the conditions in (5·23) give us the following four mutually exclusive subcases.

Case 1.1. $a_3 \equiv c_3 \equiv 0 \pmod{p}$ and $b_2 \equiv d_2 \equiv 0 \pmod{p}$.

In this case, (5·25) reduces to the system

$$\left.\begin{aligned} a_1'\alpha + a_2\beta_1 &\equiv c_1'\alpha\beta_2 + d_1\alpha\beta_3 \pmod{p} \\ a_2 &\equiv c_2\alpha \pmod{p} \\ b_1 &\equiv d_1\gamma_3 \pmod{p} \end{aligned}\right\} \tag{5·26}$$

and so the second and third equations of (5·26) together with the conditions (5·23) give us the following four mutually exclusive subcases of case 1.1

Case 1.1.1. $a_2 \equiv c_2 \equiv 0 \pmod{p}$ and $b_1 \equiv d_1 \equiv 0 \pmod{p}$.

In this case the condition for $\sigma \sim \tau$ is given by (5·23) and $a_1' \equiv c_1'\beta_2 \pmod{p}$. This has a solution if and only if $a_1' \equiv c_1' \equiv 0 \pmod{p}$ or $a_1', c_1' \not\equiv 0 \pmod{p}$, and so we have two distinct $\sim$-classes in this case with representatives

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 0 & 0 \\ p & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Case 1.1.2. $a_2 \equiv c_2 \equiv 0 \pmod{p}$ and $b_1, d_1 \not\equiv 0 \pmod{p}$.

In this case the condition for $\sigma \sim \tau$ is given by (5·23) and

$$\begin{aligned} a_1' &\equiv c_1'\beta_2 + d_1\beta_3 \pmod{p} \\ b_1 &\equiv d_1\gamma_3 \pmod{p} \end{aligned}$$

The second equation here defines γ_3 and then choosing arbitrary values for α and β_2 subject to the conditions (5·23) we can choose β_3 to solve the first congruence here. Hence there is one $\sim$-class here with representative

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ p & 0 & 0 \end{pmatrix}.$$

Case 1.1.3. $a_2, c_2 \not\equiv 0 \pmod{p}$ and $b_1 \equiv d_1 \equiv 0 \pmod{p}$.

In this case the condition for $\sigma \sim \tau$ is given by (5·23) together with

$$\begin{aligned} a_1'\alpha + a_2\beta_1 &\equiv c_1'\alpha\beta_2 \pmod{p} \\ a_2 &\equiv c_2\alpha \pmod{p} \end{aligned}$$

and this system always has a solution. Therefore we have one $\sim$–class here with representative

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Case 1.1.4. $a_2, c_2 \not\equiv 0 \pmod{p}$ and $b_1, d_1 \not\equiv 0 \pmod{p}$.

In this case, γ_3 and α are defined uniquely by the second and third equation of (5·26), and then choosing β_2 arbitrarily subject to (5·23) we can choose β_1 and β_3 to solve the first equation of (5·26). Hence there is one $\sim$–class in this case with representative

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & p & 0 \\ p & 0 & 0 \end{pmatrix}.$$

Case 1.2. $a_3 \equiv c_3 \equiv 0 \pmod{p}$ and $b_2, d_2 \not\equiv 0 \pmod{p}$.

Recall that the condition for $\sigma \sim \tau$ is given by (5·23) together with (5·25) where $a_3 \equiv c_3 \equiv 0 \pmod{p}$. We first show that there are at most two $\sim$–classes in this case by looking at the determinant of the matrix

$$S = \begin{pmatrix} c_1' & d_1 \\ c_2 & d_2 \end{pmatrix}.$$

Suppose first that $\det S \equiv 0 \pmod{p}$ and that σ is taken to be the derivation in the present case with $a_1' \equiv a_2 \equiv b_1 \equiv 0 \pmod{p}$ and $b_2 \equiv 1 \pmod{p}$. Then since $d_2 \not\equiv 0 \pmod{p}$ the condition on the determinant shows that the first congruence in (5·25) is a multiple of the second and so can be ignored. Therefore $\sigma \sim \tau$ if and only if the system consisting of (5·23) together with the following congruences have a solution

$$\begin{aligned} c_2\beta_2 + d_2\beta_3 &\equiv 0 \pmod{p} \\ d_1\alpha\gamma_3 &\equiv \beta_1 \pmod{p} \\ d_2\alpha\gamma_3 &\equiv \beta_2 \pmod{p} \end{aligned}$$

and this is always the case (using the fact that $d_2 \not\equiv 0 \pmod{p}$). So when $\det S \equiv 0 \pmod{p}$, we have shown that $\tau \sim \rho_1$ where $\rho_1 = \sigma$, i.e.

$$\rho_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & p & 0 \end{pmatrix}.$$

Now suppose that $\det S \not\equiv 0 \pmod{p}$ and that σ is the derivation in the present case with $a_1' \equiv 0 \pmod{p}$ and $a_2 \equiv b_1 \equiv b_2 \equiv 1 \pmod{p}$. The condition that $\sigma \sim \tau$ is then given by (5·23) together with the following system

$$\left.\begin{aligned} \beta_1 &\equiv c_1'\alpha\beta_2 + d_1\alpha\beta_3 \pmod{p} \\ \beta_2 &\equiv c_2\alpha\beta_2 + d_2\alpha\beta_3 \pmod{p} \end{aligned}\right\} \tag{5·27}$$

$$\left.\begin{aligned} \alpha + \beta_1 &\equiv d_1\alpha\gamma_3 \pmod{p} \\ \beta_2 &\equiv d_2\alpha\gamma_3 \pmod{p} \end{aligned}\right\} \tag{5·28}$$

Using (5·28) we can replace (5·27) with the congruences

$$\left.\begin{aligned} d_1\gamma_3 - 1 &\equiv c_1'\beta_2 + d_1\beta_3 \pmod{p} \\ d_2\gamma_3 &\equiv c_2\beta_2 + d_2\beta_3 \pmod{p} \end{aligned}\right\} \tag{5·29}$$

Now the determinant condition implies that for any value of γ_3, (5·29) has a unique solution for β_2 and β_3 and it is easy to see that $\beta_2 \not\equiv 0 \pmod{p}$ (a contradiction arises otherwise using the fact that d_2 is coprime to p). Therefore choosing $\gamma_3 \not\equiv 0 \pmod{p}$ we obtain $\beta_2 \not\equiv 0 \pmod{p}$ and then we can always obtain a solution to (5·23) together with (5·28). Hence we have shown that when $\det S$ is coprime to p we have $\tau \sim \rho_2$ where $\rho_2 = \sigma$, i.e.

$$\rho_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & p & 0 \\ p & p & 0 \end{pmatrix}.$$

So in this case there are at most two $\sim$-classes with repesentatives ρ_1 and ρ_2. But it is easy to see that ρ_1 is not $\sim$- equivalent to ρ_2 since otherwise, from the defining conditions (5·3) for the relation $\sim$, this would imply that the Lie ring $X^{\rho_1}_{e_{n-3}}$ is isomorphic to $X^{\rho_2}_{e_{n-3}}$ (the notation here is defined in (4·6) of the previous chapter). But this cannot be the case since in $X^{\rho_1}_{z,\, e_{n-3}}$ the derived subring has order p (being equal to $\langle pu_1 \rangle$ under the appropriate identifications), whereas in $X^{\rho_2}_{z,\, e_{n-3}}$ the derived subring has order p^2 (being equal to

$\langle pz \rangle \oplus \langle pu_1 \rangle$). Therefore there are two distinct $\sim$–classes in this case with representatives ρ_1 and ρ_2.

Case 1.3. $a_3, c_3 \not\equiv 0 \pmod{p}$ and $b_2 \equiv d_2 \equiv 0 \pmod{p}$.

From (5·25) we see that in this case $\sigma \sim \tau$ if and only if (5·23) together with the following system has a solution

$$\begin{aligned} a_1'\alpha + a_2\beta_1 + a_3\gamma_1 &\equiv c_1'\alpha\beta_2 + d_1\alpha\beta_3 \pmod{p} \\ a_2\beta_2 + a_3\gamma_2 &\equiv c_2\alpha\beta_2 \pmod{p} \\ a_3\gamma_3 &\equiv c_3\alpha\beta_2 \pmod{p} \\ b_1 &\equiv d_1\gamma_3 \pmod{p} \end{aligned}$$

Now if we have a solution to (5·23) and the third and fourth equations of this system then γ_1 and γ_2 can be chosen to obtain a solution to the whole system. Therefore the first two equations can be ignored, and from the fourth equation we see that a solution is obtainable only if $b_1 \equiv d_1 \equiv 0 \pmod{p}$ or $b_1, d_1 \not\equiv 0 \pmod{p}$, and either of these is seen to be sufficient also. Hence there are two $\sim$–classes in this case with representatives

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ p & 0 & 0 \end{pmatrix}.$$

Case 1.4. $a_3, c_3 \not\equiv 0 \pmod{p}$ and $b_2, d_2 \not\equiv 0 \pmod{p}$.

In this case the condition that $\sigma \sim \tau$ is given by (5·23) together with the full system (5·25), but since a_3 and b_2 are coprime to p, we can ignore the first, second and fourth equations of (5·25) (we can choose γ_1, γ_2 and β_1 to solve these once solutions to the others are found). Therefore (5·25) reduces to

$$\left.\begin{aligned} a_3\gamma_3 &\equiv c_3\alpha\beta_2 \pmod{p} \\ b_2\beta_2 &\equiv d_2\alpha\gamma_3 \pmod{p} \end{aligned}\right\} \tag{5·30}$$

Using the second equation to substitute for α, the first equation becomes

$$a_3c_3^{-1}d_2b_2^{-1} \equiv \beta_2^2\gamma_3^{-2} \pmod{p}$$

and this equation is soluble if and only if a_3c_3 and d_2b_2 have the same quadratic character modulo p. If this condition is satisfied then a solution to (5·23) and (5·30) can be obtained and so there are two distinct $\sim$–classes in this case with representatives (for ν a fixed non-quadratic residue modulo p)

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & p & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & p\nu & 0 \end{pmatrix}.$$

So summarising, in case 1 there are 11 distinct $\sim$–classes. We now deal with case 2.

Case 2 $a_1, c_1 \not\equiv 0 \pmod{p}$.

Recall that the condition for $\sigma \sim \tau$ in this case is given by (5·23) and (5·24), and using (5·23) we see that the first equation in (5·24) implies that we must have $\beta_2 \equiv a_1c_1^{-1} \pmod{p}$. With this constraint on β_2 it follows that if we have a solution to the last four equations of (5·24) subject to the conditions in (5·23) then we can lift β_2 to give a solution to the first equation of (5·24). Hence the first equation of (5·24) can be ignored provided we keep this constraint on β_2, and so the system we consider is

$$\left.\begin{aligned} \alpha\,,\,\beta_2\,,\,\gamma_3 &\not\equiv 0 \pmod{p} \\ \beta_2 &\equiv a_1c_1^{-1} \pmod{p} \end{aligned}\right\} \tag{5·31}$$

$$\left.\begin{aligned} a_2\beta_2 + a_3\gamma_2 &\equiv \alpha\beta_2c_2 + \alpha\beta_3d_2 \pmod{p} \\ a_3\gamma_3 &\equiv \beta_2\alpha c_3 \pmod{p} \\ b_1\alpha + b_2\beta_1 &\equiv \alpha\gamma_2c_1 + \alpha\gamma_3d_1 \pmod{p} \\ b_2\beta_2 &\equiv d_2\alpha\gamma_3 \pmod{p} \end{aligned}\right\} \tag{5·32}$$

From the second and fourth equations of (5·32) we have the following four mutually exclusive subcases.

Case 2.1. $a_3 \equiv c_3 \equiv 0 \pmod{p}$ and $b_2 \equiv d_2 \equiv 0 \pmod{p}$.

In this case the system (5·32) reduces to

$$\begin{aligned} a_2 &\equiv c_2\alpha \pmod{p} \\ b_1 &\equiv c_1\gamma_2 + d_1\gamma_3 \pmod{p} \end{aligned}$$

Hence we must have $a_2 \equiv c_2 \equiv 0 \pmod{p}$ or $a_2, c_2 \not\equiv 0 \pmod{p}$, and it is clear that either of these is sufficient also so that there are two distinct $\sim$–classes with representatives

$$\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 0 & 0 \\ 1 & p & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Case 2.2. $a_3 \equiv c_3 \equiv 0 \pmod{p}$ and $b_2, d_2 \not\equiv 0 \pmod{p}$.

In this case (5·32) reduces to

$$\begin{aligned} a_2\beta_2 &\equiv \alpha\beta_2 c_2 + \alpha\beta_3 d_2 \pmod{p} \\ b_1\alpha + b_2\beta_1 &\equiv \alpha\gamma_2 c_1 + \alpha\gamma_3 d_1 \pmod{p} \\ b_2\beta_2 &\equiv d_2\alpha\gamma_3 \pmod{p} \end{aligned}$$

Choosing $\gamma_3 \not\equiv 0 \pmod{p}$ arbitrarily, the third equation together with (5·31) defines α, and then γ_2 and β_3 can be chosen to give a solution to the first two equations of this system. Hence there is one $\sim$–class in this case with representative

$$\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & p & 0 \end{pmatrix}.$$

Case 2.3. $a_3, c_3 \not\equiv 0 \pmod{p}$ and $b_2 \equiv d_2 \equiv 0 \pmod{p}$.

In this case the condition that $\sigma \sim \tau$ is given by (5·31) together with (5·32) where we take $b_2 \equiv d_2 \equiv 0 \pmod{p}$. We first consider the situation in this subcase where $a_2 \equiv c_2 \equiv 0 \pmod{p}$. The condition for $\sigma \sim \tau$ is then given by (5·31) together with

$$\begin{aligned} a_3\gamma_2 &\equiv 0 \pmod{p} \\ a_3\gamma_3 &\equiv \beta_2\alpha c_3 \pmod{p} \\ b_1\alpha &\equiv \alpha\gamma_2 c_1 + \alpha\gamma_3 d_1 \pmod{p} \end{aligned}$$

which is soluble only if $b_1 \equiv d_1 \equiv 0 \pmod{p}$ or $b_1, d_1 \not\equiv 0 \pmod{p}$. If either of these holds then we can solve the above system and so there are at least two $\sim$– classes in this subcase with representatives κ_1 and κ_2 given by

$$\kappa_1 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \kappa_2 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ p & 0 & 0 \end{pmatrix}.$$

We now show that there are exactly two $\sim$–classes by letting τ be a derivation in this subcase with $c_2 \not\equiv 0 \pmod{p}$ and deducing that $\tau \sim \kappa_1$ or $\tau \sim \kappa_2$. So let τ be such a derivation and suppose first that $c_3d_1 + c_2c_1 \equiv 0 \pmod{p}$. Then if we let σ be the derivation κ_1 (so that $a_1 \equiv a_3 \equiv 1 \pmod{p}$ and $a_2 \equiv b_1 \equiv 0 \pmod{p}$) we see that $\tau \sim \kappa_1$ if and only if (5·31) and the following have a solution

$$\left.\begin{aligned} \gamma_2 &\equiv \alpha\beta_2 c_2 \pmod{p} \\ \gamma_3 &\equiv \beta_2\alpha c_3 \pmod{p} \end{aligned}\right\} \qquad (5\cdot33)$$
$$c_1\gamma_2 + d_1\gamma_3 \equiv 0 \pmod{p}$$

The third equation will follow automatically from a solution to (5·33) since we are assuming that $c_3d_1 + c_2c_1 \equiv 0 \pmod{p}$, and so since (5·33) together with (5·31) is always soluble, it follows that $\tau \sim \kappa_1$.

Now suppose that $c_3d_1 + c_2c_1 \not\equiv 0 \pmod{p}$ and let σ be the derivation κ_2 (so that $a_1 \equiv a_3 \equiv b_1 \equiv 1 \pmod{p}$ and $a_2 \equiv 0 \pmod{p}$). The condition for $\tau \sim \kappa_2$ is therefore given by (5·31) together with (5·33) and the equation

$$c_1\gamma_2 + d_1\gamma_3 \equiv 1 \pmod{p}.$$

Now use (5·33) to see that this equation is equivalent to $\alpha^{-1} \equiv \beta_2(c_3d_1 + c_2c_1) \pmod{p}$, and since the constraint on β_2 in (5·31) ensures that the right-hand side of this is coprime to p, it follows that the above system always has a solution. Hence $\tau \sim \kappa_2$ and so in this subcase there are two distinct $\sim$–classes with representatives κ_1 and κ_2.

Case 2.4. $a_3, c_3 \not\equiv 0 \pmod{p}$ and $b_2, d_2 \not\equiv 0 \pmod{p}$.

In this case the condition for $\sigma \sim \tau$ is given by the full system (5·31) and (5·32), and given a solution to the second and fourth equations of (5·32) together with the conditions in (5·31), we can choose β_1 and β_3 to obtain solutions to the whole system (using the fact that b_2 and d_2 are coprime to p). Therefore we can ignore the first and third equations of (5·32), and using the fourth equation of (5·32) to substitute for α we can replace the second equation of (5·32) by

$$a_3b_2^{-1}c_3^{-1}d_2 \equiv \beta_2^2\gamma_3^{-2} \pmod{p}$$

which shows that $\sigma \sim \tau$ only if $a_3 b_2$ and $c_3 d_2$ have the same quadratic character modulo p. If either of these conditions holds then we can always obtain a solution to (5·31) and (5·32), and so there are two distinct $\sim$–classes in this subcase with representatives (ν denotes a fixed non-quadratic residue modulo p)

$$\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & p & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & p\nu & 0 \end{pmatrix}.$$

So summarising, in case 2 we have shown that there are 7 distinct $\sim$– classes and so together with case 1 we see that $\Delta^p_{n-3}(2,1,\boldsymbol{X}) = 11 + 7 = 18$.

Section 5·2·5. Summary.

In the previous three subsections we showed that for a prime p greater than 3 and a natural number n greater than 6

$$\begin{aligned} \Delta^p_{n-3}(2,1,\boldsymbol{V}) &= 2p+1 \\ \Delta^p_{n-3}(2,1,\boldsymbol{W}) &= 3p+11 \\ \Delta^p_{n-3}(2,1,\boldsymbol{X}) &= 18 \end{aligned}$$

and so by (5·1) we see that

$$\Delta^p_{n-3}(2,1) = 5p+30$$

from which it follows that

$$\Psi^p_{n-3}(2,1) = 5p+30\,.$$

Section 5·3. The Calculation of $\Psi^p_{n-3}(3)$ for $p \geq 5$ and $n \geq 7$.

Recall from theorem 4·10 that for $p \geq 5$ and $n \geq 7$, $\Psi^p_{n-3}(3)$ equals the number of isomorphism classes $\Delta^p_{n-3}(3)$ of nilpotent Lie rings in $\mathcal{F}^p_{n-3}(3)$, and that this number is independent of n for $n \geq 9$. In section 5·3·1 we show how to calculate $\Delta^p_4(3)$ by classifying directly the nilpotent Lie ring structures on a fixed Abelian p-group of ***type***$(4,3)$. Using exactly the same technique we have calculated the nilpotent Lie ring structures on fixed Abelian p-groups of ***type***$(5,3)$ and ***type***$(n-3,3)$ for $n \geq 9$ thereby calculating $\Delta^p_5(3)$ and $\Delta^p_{n-3}(3)$, and since the technique is so similar we just include a list of isomorphism representatives in either case (these are presented in section 5·3·2).

Section 5·3·1. Calculation of $\Delta^p_{n-3}(3)$ for n Equal to 7.

In this section we assume that p is a fixed prime greater than or equal to 5. Let A denote the fixed Abelian p-group of *type* $(4,3)$ given by

$$A = \left(\mathbb{Z}/p^4\mathbb{Z}\right)u \ \oplus \left(\mathbb{Z}/p^3\mathbb{Z}\right)v\,.$$

Now any Lie ring structure on A is uniquely determined by the value of $[u,v]$ since all other brackets follow from this and the Lie ring axioms, and since v has order p^3 we must have $[u,v] \in \Omega_3(A) = \langle pu\rangle \oplus \langle v\rangle$. Conversely, given any element $a \in \Omega_3(A)$ there is a unique ring structure on A with $[u,v] = a$ and $[x,x] = 0$ for any $x \in A$, and in such a ring it is easy to see that the Jacobi identity automatically holds. Nilpotency in such a Lie ring is equivalent to $[u,v] \in \mathfrak{U}_1(A)$, and so it follows that the nilpotent Lie ring structures L on A are given by

$$[u,v]_L = \alpha pu + \beta pv \quad \text{where } \alpha,\beta \in \mathbb{Z}\,.$$

We now determine isomorphism class representatives by using the fact that the derived subring of such a Lie ring is just the cyclic subgroup of A generated by $[u,v]$. Note that for an integer γ coprime to p we denote by γ^{-1} any integer such that $\gamma\gamma^{-1} \equiv 1 \pmod{p^4}$.

Case 1. Lie rings L on A with $\left|[L,L]\right| = p^3$.

Letting $[u,v]_L = \alpha pu + \beta pv$ we must have $\alpha \not\equiv 0 \pmod{p}$, and so taking the basis of A to be u', v' where $u' = u + \alpha^{-1}\beta v,\ v' = \alpha^{-1}v$ we see that $[u',v'] = pu'$ so that L is isomorphic to the Lie ring L_{1a} on A given by

$$[u,v]_{L_{1a}} = pu.$$

Therefore there is one isomorphism class in this case.

Case 2. Lie rings L on A with $\left|[L,L]\right| = p^2$.

Let $[u,v]_L = \alpha p^2 u + \beta pv$. If $\beta \equiv 0 \pmod{p}$ then we must have $\alpha \not\equiv 0 \pmod{p}$, and writing $\beta = p\gamma$ we have a basis $u' = u + \alpha^{-1}\gamma v,\ v' = \alpha^{-1}v$ of A where $[u',v'] = p^2u'$, so that L is isomorphic to the Lie ring L_{2a} on A given by

$$[u,v]_{L_{2a}} = p^2u.$$

If $\beta \not\equiv 0 \pmod{p}$ then taking the basis to be $u' = \beta^{-1}u$, $v' = \alpha\beta^{-1}pu + v$ we see that L is isomorphic to the Lie ring L_{2b} on A given by

$$[u, v]_{L_{2b}} = pv.$$

Now $L_{2a} \not\cong L_{2b}$ since $[L_{2a}, L_{2a}] \subseteq \mathfrak{U}_2(A)$ whereas $[L_{2b}, L_{2b}] \not\subseteq \mathfrak{U}_2(A)$, so there are two isomorphism classes in this case.

Case 3. Lie rings L on A with $|[L, L]| = p$.

Let $[u, v]_L = \alpha p^3 u + \beta p^2 v$. If $\beta \equiv 0 \pmod{p}$ then we must have $\alpha \not\equiv 0 \pmod{p}$, and so taking $u' = u$, $v' = \alpha^{-1}v$ we see that L is isomorphic to the Lie ring L_{3a} on A given by

$$[u, v]_{L_{3a}} = p^3 u.$$

If $\beta \not\equiv 0 \pmod{p}$ then taking $u' = \beta^{-1}u$, $v' = \alpha\beta^{-1}pu + v$ we see that L is isomorphic to the Lie ring L_{3b} on A given by

$$[u, v]_{L_{3b}} = p^2 v.$$

Now $L_{3a} \not\cong L_{3b}$ since $[L_{3a}.L_{3a}] \subseteq \mathfrak{U}_3(A)$ whereas $[L_{3b}, L_{3b}] \not\subseteq \mathfrak{U}_3(A)$, so there are two isomorphism classes in this case.

Case 4. Lie rings L on A with $|[L, L]| = 1$.

There is one structure here given by $[u, v] = 0$.

So summarising the above, we have shown that $\Delta_4^p(3) = 6$ for $p \geq 5$.

Section 5·3·2. Summary of $\Delta^p_{n-3}(3)$ for $n \geq 8$.

For $p \geq 5$ and $n \geq 8$ the procedure used in section 5·3·1 can be applied to the Abelian p-group

$$\left(\mathbb{Z}/_{p^{n-3}\mathbb{Z}}\right) u \oplus \left(\mathbb{Z}/_{p^3\mathbb{Z}}\right) v$$

to calculate $\Delta^p_{n-3}(3)$ by using the order of the derived subring as an invariant to determine a set of isomorphism representatives for the nilpotent Lie ring structures. We have carried out these calculations and summarise them here by giving the defining bracket between the basis elements u and v for each isomorphism representative. The cases $n = 8$ and $n \geq 9$ are given separately.

The case n equals 8

1. Representatives with derived subring of order p^3
   - a) $[u, v] = p^2 u$
   - b) $[u, v] = p^2 u + pv$
2. Representatives with derived subring of order p^2
   - a) $[u, v] = p^3 u$
   - b) $[u, v] = p^3 u + p^2 v$
   - c) $[u, v] = pv$
3. Representatives with derived subring of order p or 1
   - a) $[u, v] = p^4 u$
   - b) $[u, v] = p^2 v$
   - c) $[u, v] = 0$

So for $p \geq 5$ we see that $\Delta^p_8(3) = 8$.

The case n greater than 8

1. Representatives with derived subring of order p^3

   a) $[u,v] = p^{n-6}u$

   b) $[u,v] = p^{n-6}u + p^2v$

   c) $[u,v] = p^{n-6}u + pv$

2. Representatives with derived subring of order p^2

   a) $[u,v] = p^{n-5}u$

   b) $[u,v] = p^{n-5}u + p^2v$

   c) $[u,v] = pv$

3. Representatives with derived subring of order p or 1

   a) $[u,v] = p^{n-4}u$

   b) $[u,v] = p^2v$

   c) $[u,v] = 0$

So for $p \geq 5$ and $n \geq 9$ we see that $\Delta_9^p(3) = 9$.

Chapter 6. A Connection Between $\mathbb{F}_p[T]$- Lie Algebras and Finite p-Groups

Section 6·1. Introduction.

In this chapter we provide an affirmative solution to a restricted form of the following conjecture of J. Moody [22]

Conjecture. ([22]) *For each natural number n and for all but finitely many primes p (the excluded primes depending on n), there is a non-natural one-to-one correspondence between isomorphism classes of groups of order p^n and isomorphism classes of nilpotent $\mathbb{F}_p[T]/(T^n)-$Lie algebras of $\mathbb{F}_p-$dimension n.*

The context in which we consider this conjecture is for finite p-groups satisfying the additional hypothesis that their derived subgroup has exponent dividing p, and we show that by restricting the Lie algebras accordingly, a positive solution can be obtained under these conditions. Specifically, we will show the following theorem.

Theorem 6·1. *Let n be a natural number and suppose that p is a prime greater than or equal to n. Then there exists a natural, but not functorial, one-to-one correspondence between the isomorphism classes of groups of order p^n whose derived subgroup has exponent dividing p, and the isomorphism classes of nilpotent $\mathbb{F}_p[T]/(T^n)-$Lie algebras L of $\mathbb{F}_p-$dimension n in which $T[L,L]=0$.*

The correspondence we give is explicit although is not a functorial isomorphism since information concerning the morphisms of the respective categories is lost in the transition. We show that this is the case by considering automorphism groups of certain objects.

The approach we take to prove this theorem is to use the natural Lie ring correspondence (given by the Campbell-Hausdorff formula – see section 1·1·3) associated with groups of order p^n (for $p \geq n$) to translate the problem into a question about certain finite Lie rings of order p^n, and then establish the connection between this category and

the category of Lie algebras in the statement of the theorem. The proof of this result is necessarily careful due to the fact that the correspondence we establish is not functorial.

Now since an $\mathsf{F}_p[T]/(T^n)-$Lie algebra L has an underlying F_p-Lie algebra (by ignoring the $T-$action), it follows that in the situation when $p \geq n$, the Campbell-Hausdorff formula can be used again to recover a group of exponent p and order p^n. Using this observation, one can then use theorem 6·1 to obtain a "formula" for the number of groups of order p^n which have exponent p derived subgroup. Denoting by $\mathcal{E}_n^p$ a transversal for the isomorphism classes of groups of order p^n and exponent p, and for such a group E, letting N_E denote the endomorphisms $\sigma : E \to E$ with the property that $\operatorname{Im}\sigma \subseteq Z(E)$ and $\sigma^n = e_E$ (the endomorphism of E sending the entire group to the identity), the formula we obtain is the following

Theorem 6·2. *For a natural number n and a prime p greater than or equal to n, the number of isomorphism classes of groups of order p^n whose derived subgroup has exponent dividing p is given by*

$$\sum_{E \in \mathcal{E}_n^p} \sum_{\phi \in N_E} \frac{1}{\left| \phi^{\operatorname{Aut}(E)} \right|},$$

where $\operatorname{Aut}(E)$ acts on N_E by conjugation.

So once a classification is obtained for the groups of order p^n and exponent p, for fixed $p \geq n$ (or equivalently, a classification of the nilpotent F_p-Lie algebras of F_p-dimension n), we automatically have information about the groups of order p^n whose derived subgroup has exponent dividing p. In particular, this remark applies in the case of groups of order p^7 since Wilkinson [30] has published a summary list of his classification of groups of order p^7 and exponent p. We return to this in section 6·4.

The approach of using modular Lie algebras to derive information about finite p-groups is currently being used to solve some important questions. For instance, Shalev [27] proves the coclass Conjecture A of Leedham-Green and Newman [16] and obtains an explicit bound for the function $f(p,r)$ of the conjecture by using such a modular approach. The method is essentially to assume the conjecture is false and then use the $p^{\text{th}}-$power map in a counterexample to put an $\mathsf{F}_p[T]-$Lie algebra structure on the associated standard

graded Lie ring tensored with F_p (this graded construction was described briefly in section 1·1·1). The resulting Lie algebra is then used to construct a non-trivial nilpotent perfect Lie algebra thus obtaining the desired contradiction.

Having said this however, it should be noted that the nilpotent n-dimensional F_p-Lie algebra which we associate to each isomorphism class of groups of order p^n ($p \geq n$) whose derived subgroup has exponent dividing p (obtained by ignoring the $T-$action) is **not**, in general, the graded Lie algebra which arises from the filtration of such a group by the lower p-central series. This follows from the fact that for groups of exponent p, the F_p-Lie algebra we associate is isomorphic to the Lie algebra given by the Campbell-Hausdorff formula and this Lie algebra is uniquely determined by the isomorphism type of the group. This is not the case for the graded construction however, since one always has non-isomorphic groups of order p^n ($p, n \geq 5$) whose F_p-Lie algebras arising from the lower p-central series are isomorphic. To see that this is the case, consider the table of groups of order p^5 given in [12] and in particular the groups (in the notation of the paper) $\phi_9(1^5)$ and $\phi_{10}(1^5)$. These are both of exponent p, maximal class 4 and non-isoclinic (hence non-isomorphic), but from the presentations given there one can verify that the 5-dimensional graded F_p-Lie algebras arising from their lower central series are both isomorphic to the split extension of the 4-dimensional Abelian F_p-Lie algebra by a nilpotent linear map of maximum nilpotency class 4 (for $p \geq 5$). By taking direct products of these two groups with an elementary Abelian p-group of the appropriate order one sees that a similar situation holds for any $n \geq 5$.

Section 6·2. A Connection Between Certain Rings and Algebras.

If C is any commutative ring with 1 then recall from section 1·1·1 that we define a C-algebra to be a unital C-module A equipped with an element of $\mathrm{Hom}_C(A \otimes_C A, A)$ giving the multiplication in A (such a multiplication is denoted by a bracket $[.,.]$). In this context, a ring will be taken to mean a $\mathbb{Z}-$algebra.

In this section we establish, for an arbitrary prime p and natural number n, a one-to-one correspondence between the family $\mathcal{R}_n^p$ of rings R of order p^n in which $p[R,R] = 0$, and the family $\mathcal{A}_n^p$ of $\mathsf{F}_p[T]/(T^n)-$algebras A of F_p-dimension n in which $T[A,A] = 0$. In order to obtain this result we first need a few remarks about type invariants.

If A is an algebra in $\mathcal{A}_n^p$ then since T acts nilpotently it follows that there exists a partition $\mu_1 \geq \cdots \geq \mu_\omega$ of n such that the underlying $\mathsf{F}_p[T]-$module of A is isomorphic to the $\mathsf{F}_p[T]-$module

$$V = \mathsf{F}_p[T]/_{(T^{\mu_1})} \oplus \mathsf{F}_p[T]/_{(T^{\mu_2})} \oplus \cdots \oplus \mathsf{F}_p[T]/_{(T^{\mu_\omega})},$$

and we will say that A (or V) is of *type* $(\mu_1, \ldots, \mu_\omega)$. These invariants are uniquely determined by the isomorphism type of the module, as is the case for Abelian p-groups. We also define the $\Omega-$ and $\mho-$ series of such a module V in the obvious way, viz.

$$\Omega_i(V) = \{x \in V : T^i x = 0\} \quad \text{and} \quad \mho_i(V) = \{T^i x : x \in V\} \quad \text{for each integer } i \geq 0,$$

and this defines chains of ideals of any $\mathsf{F}_p[T]-$algebra structure on V. The $\Omega-$ series can then be used to define a sequence of $\omega-$invariants of such a module (as with regular p-groups – see section 1·2), and by identifying the module with an Abelian p-group of the same type in the obvious way so that the $\Omega-$ and $\mho-$ series coincide, we see that the $\mu-$invariants and the $\omega-$invariants are dual partitions of n.

We now use these type invariants to divide up the correspondence which we wish to establish. If we let $\lambda_1 \geq \cdots \geq \lambda_t$ be a partition of n, then we denote by $\mathcal{R}_n^p(\lambda_1, \ldots, \lambda_t)$ the rings in $\mathcal{R}_n^p$ of *type* $(\lambda_1, \ldots, \lambda_t)$, and similarly we denote by $\mathcal{A}_n^p(\lambda_1, \ldots, \lambda_t)$ the algebras in $\mathcal{A}_n^p$ of *type* $(\lambda_1, \ldots, \lambda_t)$. We now show the following result.

Theorem 6.3. *Let p be a prime, n be a natural number, and suppose that $\lambda_1 \geq \cdots \geq \lambda_t$ is a partition of n. Then if U is an Abelian p−group of type $(\lambda_1, \ldots, \lambda_t)$ and V is an $\mathsf{F}_p[T]/(T^n)$− module of type $(\lambda_1, \ldots, \lambda_t)$, there is a one-to-one correspondence between the isomorphism classes of rings defined on U which belong to $\mathcal{R}_n^p(\lambda_1, \ldots, \lambda_t)$, and the isomorphism classes of $\mathsf{F}_p[T]/(T^n)$−algebras defined on V which belong to $\mathcal{A}_n^p(\lambda_1, \ldots, \lambda_t)$.*

Proof. Let U and V be as in the statement of the theorem and observe that a ring R defined on U with $\Omega_1([R,R]) = 0$ is given by a unique element ϵ_R of $\mathrm{Hom}_{\mathbf{Z}}(U \otimes_{\mathbf{Z}} U, \Omega_1(U))$, and an $\mathsf{F}_p[T]$−algebra A defined on V with $\Omega_1([A,A])$ is given by a unique element γ_A of $\mathrm{Hom}_{\mathsf{F}_p[T]}(V \otimes_{\mathsf{F}_p[T]} V, \Omega_1(V))$. Then since $\mathrm{Im}\,\epsilon_R \subseteq \Omega_1(U)$ and $\mathrm{Im}\,\gamma_A \subseteq \Omega_1(V)$, it follows that $\mho_1(U \otimes_{\mathbf{Z}} U) \subseteq \ker \epsilon_R$ and $\mho_1(V \otimes_{\mathsf{F}_p[T]} V) \subseteq \ker \gamma_A$, and so using the canonical isomorphisms

$$\begin{aligned} \phi \;:\; & {}^{(U \otimes_{\mathbf{Z}} U)}\!/_{\mho_1(U \otimes_{\mathbf{Z}} U)} \longrightarrow {}^{U}\!/_{\mho_1(U)} \otimes_{\mathbf{Z}} {}^{U}\!/_{\mho_1(U)} \\ \psi \;:\; & {}^{(V \otimes_{\mathsf{F}_p[T]} V)}\!/_{\mho_1(V \otimes_{\mathsf{F}_p[T]} V)} \longrightarrow {}^{V}\!/_{\mho_1(V)} \otimes_{\mathsf{F}_p[T]} {}^{V}\!/_{\mho_1(V)} \end{aligned}$$

and using bars to indicate "modulo $\mho_1$" of the appropriate module, we see that there exist unique elements $\widehat{\epsilon}_R \in \mathrm{Hom}_{\mathbf{Z}}(\overline{U} \otimes_{\mathbf{Z}} \overline{U}, \Omega_1(U))$ and $\widehat{\gamma}_A \in \mathrm{Hom}_{\mathsf{F}_p[T]}(\overline{V} \otimes_{\mathsf{F}_p[T]} \overline{V}, \Omega_1(V))$ such that the following diagrams commute

$$\begin{array}{ccc} U \otimes_{\mathbf{Z}} U & \xrightarrow{\epsilon_R} & \Omega_1(U) \\ {\scriptstyle \mathrm{nat}}\downarrow & & \uparrow{\scriptstyle \widehat{\epsilon}_R} \\ \overline{U \otimes_{\mathbf{Z}} U} & \xrightarrow[\phi]{} & \overline{U} \otimes_{\mathbf{Z}} \overline{U} \end{array} \qquad \begin{array}{ccc} V \otimes_{\mathsf{F}_p[T]} V & \xrightarrow{\gamma_A} & \Omega_1(V) \\ {\scriptstyle \mathrm{nat}}\downarrow & & \uparrow{\scriptstyle \widehat{\gamma}_A} \\ \overline{V \otimes_{\mathsf{F}_p[T]} V} & \xrightarrow[\psi]{} & \overline{V} \otimes_{\mathsf{F}_p[T]} \overline{V} \end{array}$$

Now the isomorphism classes of rings on U which we are considering are in one-to-one correspondence with the orbits of $\mathrm{Aut}_{\mathbf{Z}}(U)$ on $\mathrm{Hom}_{\mathbf{Z}}(U \otimes_{\mathbf{Z}} U, \Omega_1(U))$ where the action is given by

$$(x \otimes y)(\epsilon_R{}^{\pi}) = (x\pi^{-1} \otimes y\pi^{-1})\epsilon_R(\pi|_{\Omega_1(U)})$$

for $\epsilon_R \in \mathrm{Hom}_{\mathbf{Z}}(U \otimes_{\mathbf{Z}} U, \Omega_1(U))$, $\pi \in \mathrm{Aut}_{\mathbf{Z}}(U)$ and $x, y \in U$. Also, since $\mho_1(U)$ is invariant under all elements of $\mathrm{Aut}_{\mathbf{Z}}(U)$, we obtain an induced action of $\mathrm{Aut}_{\mathbf{Z}}(U)$ on

$\mathrm{Hom}_{\mathbf{Z}}(\overline{U} \otimes_{\mathbf{Z}} \overline{U}, \Omega_1(U))$ so that if ϵ_R , $\epsilon_S \in \mathrm{Hom}_{\mathbf{Z}}(U \otimes_{\mathbf{Z}} U, \Omega_1(U))$ then

$$\epsilon_R{}^{\pi} = \epsilon_S \quad \text{if and only if} \quad \widehat{\epsilon}_R{}^{\pi} = \widehat{\epsilon}_S.$$

Analogously, the isomorphism classes of $\mathbf{F}_p[T]-$algebras on V which we are considering are in one-to-one correspondence with the orbits of $\mathrm{Aut}_{\mathbf{F}_p[T]}(V)$ on $\mathrm{Hom}_{\mathbf{F}_p[T]}(V \otimes_{\mathbf{F}_p[T]} V, \Omega_1(V))$ where the action is given by

$$(g \otimes h)(\gamma_A{}^{\kappa}) = (g\kappa^{-1} \otimes h\kappa^{-1})\gamma_A(\kappa|_{\Omega_1(V)})$$

for $\gamma_A \in \mathrm{Hom}_{\mathbf{F}_p[T]}(V \otimes_{\mathbf{F}_p[T]} V, \Omega_1(V))$, $\kappa \in \mathrm{Aut}_{\mathbf{F}_p[T]}(V)$ and $g, h \in V$. Also, since $\Omega_1(V)$ is invariant under $\mathrm{Aut}_{\mathbf{F}_p[T]}(V)$ we have an induced action on $\mathrm{Hom}_{\mathbf{F}_p[T]}(\overline{V} \otimes_{\mathbf{F}_p[T]} \overline{V}, \Omega_1(V))$ so that if $\gamma_A, \gamma_B \in \mathrm{Hom}_{\mathbf{F}_p[T]}(\overline{V} \otimes_{\mathbf{F}_p[T]} \overline{V}, \Omega_1(V))$ then

$$\gamma_A{}^{\kappa} = \gamma_B \quad \text{if and only if} \quad \widehat{\gamma}_A{}^{\kappa} = \widehat{\gamma}_B.$$

To complete the proof, it therefore suffices to show that there is a one-to-one correspondence between the $\mathrm{Aut}_{\mathbf{Z}}(U)-$orbits on $\mathrm{Hom}_{\mathbf{Z}}(\overline{U} \otimes_{\mathbf{Z}} \overline{U}, \Omega_1(U))$ and the $\mathrm{Aut}_{\mathbf{F}_p[T]}(V)-$orbits on $\mathrm{Hom}_{\mathbf{F}_p[T]}(\overline{V} \otimes_{\mathbf{F}_p[T]} \overline{V}, \Omega_1(V))$.

So choosing a $\mathbf{Z}-$basis $(u_1, \ldots, u_t)$ of U and an $\mathbf{F}_p[T]-$basis $(v_1, \ldots, v_t)$ of V, both corresponding to the type invariants $(\lambda_1, \ldots, \lambda_t)$, observe that $\overline{U} \otimes_{\mathbf{Z}} \overline{U}$ and $\overline{V} \otimes_{\mathbf{F}_p[T]} \overline{V}$ are t^2-dimensional vector spaces over $\mathbf{F}_p$ with $\mathbf{F}_p-$bases

$$\{\overline{u}_i \otimes \overline{u}_j \,:\, 1 \leq i, j \leq t\} \quad \text{and} \quad \{\overline{v}_i \otimes \overline{v}_j \,:\, 1 \leq i, j \leq t\},$$

respectively, and $\Omega_1(U)$ and $\Omega_1(V)$ are $t-$dimensional $\mathbf{F}_p-$vector spaces with $\mathbf{F}_p-$bases

$$(p^{\lambda_1 - 1}u_1, \ldots, p^{\lambda_t - 1}u_t) \quad \text{and} \quad (T^{\lambda_1 - 1}v_1, \ldots, T^{\lambda_t - 1}v_t),$$

respectively. We therefore have isomorphisms φ, ν of $\mathbf{F}_p-$vector spaces where

$$\begin{array}{ccccc} \varphi & : & \overline{U} \otimes_{\mathbf{Z}} \overline{U} & \longrightarrow & \overline{V} \otimes_{\mathbf{F}_p[T]} \overline{V} \\ & & \overline{u}_i \otimes \overline{u}_j & \longmapsto & \overline{v}_i \otimes \overline{v}_j \\ & & 1 \leq i, j \leq t & & \end{array} \qquad \begin{array}{ccccc} \nu & : & \Omega_1(U) & \longrightarrow & \Omega_1(V) \\ & & p^{\lambda_i - 1}u_i & \longmapsto & T^{\lambda_i - 1}v_i \\ & & & 1 \leq i \leq t & \end{array}$$

which give rise to an $\mathbf{F}_p$−vector space isomorphism

$$\theta \ : \ \mathrm{Hom}_{\mathbf{Z}}(\overline{U} \otimes_{\mathbf{Z}} \overline{U}\,, \Omega_1(U)) \quad \longrightarrow \quad \mathrm{Hom}_{\mathbf{F}_p[T]}(\overline{V} \otimes_{\mathbf{F}_p[T]} \overline{V}\,, \Omega_1(V)) \qquad (6{\cdot}1)$$

where corresponding elements have the same matrix representation relative to the identifications given by φ and ν. We now compare the orbits of elements which correspond under θ.

First, we calculate the dimensions of the blocks appearing in the matrices of the induced actions on $\overline{U}$ and $\overline{V}$. So let $1 \leq i_1 < i_2 < \cdots < i_r \leq t$ be a sequence of integers such that $\lambda_1 = \lambda_{i_1} > \lambda_{i_2} > \cdots > \lambda_{i_r} = \lambda_t$ and where for each $j = 1, \ldots, t$ there exists some integer k_j with $1 \leq k_j \leq r$ and $\lambda_j = \lambda_{i_{k_j}}$. Now recall that the type invariants are related to the ω−invariants by the fact that they are dual partitions of n, i.e. for $1 \leq j \leq \lambda_1$, ω_j is the number of λ_l's greater than or equal to j. So if we set $d_1 = \omega_{\lambda_1}$, and for $2 \leq j \leq r$ set $d_j = \omega_{\lambda_{i_j}} - \omega_{\lambda_{i_{j-1}}}$, we see that d_j is the number of λ_l's equal to λ_{i_j}. Therefore, if $\pi \in \mathrm{Aut}_{\mathbf{Z}}(U)$ then relative to the basis of $\overline{U}$ induced from the basis $(u_1, \ldots, u_t)$, the induced element $\overline{\pi^{-1}} = \overline{\pi}^{-1}$ of $\mathrm{Aut}_{\mathbf{Z}}(\overline{U})$ is represented by a matrix of the form

$$\begin{pmatrix} M_1^{-1} & * & \cdots & * \\ 0 & M_2^{-1} & \cdots & * \\ 0 & 0 & \ddots & * \\ 0 & 0 & \cdots & M_r^{-1} \end{pmatrix} \in \mathrm{GL}_t(\mathbf{F}_p) \qquad (6{\cdot}2)$$

where $M_j \in \mathrm{GL}_{d_j}(\mathbf{F}_p)$ for each $j = 1, \ldots, r$. For the same element π and taking the basis of $\Omega_1(U)$ to be $(p^{\lambda_1 - 1}u_1, \ldots, p^{\lambda_t - 1}u_t)$, we see that $\pi|_{\Omega_1(U)}$ is represented by a matrix of the form

$$\begin{pmatrix} M_1 & 0 & \cdots & 0 \\ * & M_2 & \cdots & 0 \\ * & * & \ddots & 0 \\ * & * & \cdots & M_r \end{pmatrix} \in \mathrm{GL}_t(\mathbf{F}_p) \qquad (6{\cdot}3)$$

where the diagonal blocks are the inverses of the corresponding diagonal blocks in the representation for $\overline{\pi}^{-1}$ in (6·2). In addition, given matrices $E, F \in \mathrm{GL}_t(\mathbf{F}_p)$ where E is of

the form (6·2) and F is of the form (6·3) (where corresponding diagonal blocks are inverse to each other), there exists $\pi \in \mathrm{Aut}_{\mathbf{Z}}(U)$ with $\overline{\pi}$ represented by E and $\pi|_{\Omega_1(U)}$ represented by F.

If we now let $\kappa \in \mathrm{Aut}_{\mathbf{F}_p[T]}(V)$ then a similar situation holds. That is to say, the induced element $\overline{\kappa^{-1}} = \overline{\kappa}^{-1}$ in $\mathrm{Aut}_{\mathbf{F}_p[T]}(\overline{V})$ is represented by a matrix of the form (6·2), and the restriction $\kappa|_{\Omega_1(V)}$ is represented by a matrix of the form (6·3) with corresponding diagonal blocks inverse to each other (where the bases are taken to be induced and restricted from $(v_1, \ldots, v_t)$, respectively). Moreover, any two matrices of this form arise in this way.

It follows from the above and the identification given by θ in (6·1) that for $\widehat{\epsilon}_R, \widehat{\epsilon}_S \in \mathrm{Hom}_{\mathbf{Z}}(\overline{U} \otimes_{\mathbf{Z}} \overline{U}, \Omega_1(U))$, $\widehat{\epsilon}_R$ and $\widehat{\epsilon}_S$ are in the same $\mathrm{Aut}_{\mathbf{Z}}(U)-$ orbit if and only if $\widehat{\epsilon}_R\theta$ and $\widehat{\epsilon}_S\theta$ are in the same $\mathrm{Aut}_{\mathbf{F}_p[T]}(V)-$orbit, so that θ induces a one-to-one correspondence between orbits, as required. □

Remark. A change of basis in U or V will give rise to a different isomorphism θ', and if two orbits correspond under θ then they also correspond under θ' with θ' identifying different elements. Therefore the correspondence between orbits is independent of which basis is chosen.

Corollary 6·4. *Let p be a prime and n a natural number.*

i) For any partition $\lambda_1 \geq \cdots \geq \lambda_t$ of n, there is a one-to-one correspondence between isomorphism classes in $\mathcal{R}_n^p(\lambda_1, \ldots, \lambda_t)$ and isomorphism classes in $\mathcal{A}_n^p(\lambda_1, \ldots, \lambda_t)$.

ii) There is a one-to-one correspondence between isomorphism classes in $\mathcal{R}_p^n$ and isomorphism classes in $\mathcal{A}_n^p$.

Proof.

i) This follows immediately from theorem 6·3 and the fact that each isomorphism class in $\mathcal{R}_n^p(\lambda_1, \ldots, \lambda_t)$ determines a unique isomorphism class of rings defined on U, and each isomorphism class in $\mathcal{A}_n^p(\lambda_1, \ldots, \lambda_t)$ determines a unique isomorphism class of algebras defined on V.

ii) This follows from i) and the fact that the isomorphism classes in $\mathcal{R}_n^p$ and $\mathcal{A}_n^p$ are partitioned by the type invariants. □

Note. The proof given here depends on fixing the underlying modules U and V corresponding to the type invariants. If we choose a different module U', then there is a natural one-to-one correspondence between the $\mathrm{Aut}_{\mathbf{Z}}(U)-$ orbits on $\mathrm{Hom}_{\mathbf{Z}}(\overline{U} \otimes_{\mathbf{Z}} \overline{U}, \Omega_1(U))$ and the $\mathrm{Aut}_{\mathbf{Z}}(U')-$ orbits on $\mathrm{Hom}_{\mathbf{Z}}(\overline{U'} \otimes_{\mathbf{Z}} \overline{U'}, \Omega_1(U'))$, where corresponding orbits give isomorphic rings. Similarly, choosing a different module V' there is a natural one-to-one correspondence between the $\mathrm{Aut}_{\mathbf{F}_p[T]}(V)-$orbits on $\mathrm{Hom}_{\mathbf{F}_p[T]}(\overline{V} \otimes_{\mathbf{F}_p[T]} \overline{V}, \Omega_1(V))$ and the $\mathrm{Aut}_{\mathbf{F}_p[T]}(V')-$orbits on $\mathrm{Hom}_{\mathbf{F}_p[T]}(\overline{V'} \otimes_{\mathbf{F}_p[T]} \overline{V'}, \Omega_1(V'))$, and using the above remark (that the correspondence between isomorphism classes is independent of which bases are chosen), we therefore have a commutative diagram

$$\begin{array}{ccc} \mathrm{Hom}_{\mathbf{Z}}(\overline{U} \otimes_{\mathbf{Z}} \overline{U}, \Omega_1(U))/\mathrm{Aut}_{\mathbf{Z}}(U) & \rightarrow & \mathrm{Hom}_{\mathbf{F}_p[T]}(\overline{V} \otimes_{\mathbf{F}_p[T]} \overline{V}, \Omega_1(V))/\mathrm{Aut}_{\mathbf{F}_p[T]}(V) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{\mathbf{Z}}(\overline{U'} \otimes_{\mathbf{Z}} \overline{U'}, \Omega_1(U'))/\mathrm{Aut}_{\mathbf{Z}}(U') & \rightarrow & \mathrm{Hom}_{\mathbf{F}_p[T]}(\overline{V'} \otimes_{\mathbf{F}_p[T]} \overline{V'}, \Omega_1(V'))/\mathrm{Aut}_{\mathbf{F}_p[T]}(V') \end{array}$$

where the horizontal correspondences are given by theorem 6·3. It follows therefore that the correspondences in corollary 6·4 are independent of the underlying modules chosen.

In order to apply corollary 6·4 in the next section, we need to show that this correspondence between isomorphism classes sends isomorphism classes of nilpotent Lie rings to isomorphism classes of nilpotent $\mathbf{F}_p[T]-$Lie algebras (and vice-versa). This is the content of the following proposition.

Proposition 6·5. *The correspondence established in theorem 6·3 between isomorphism classes of rings defined on U belonging to $\mathcal{R}_n^p(\lambda_1, \ldots, \lambda_t)$, and isomorphism classes of algebras defined on V belonging to $\mathcal{A}_n^p(\lambda_1, \ldots, \lambda_t)$, sends isomorphism classes of Lie rings onto isomorphism classes of $\mathbf{F}_p[T]/(T^n)-$Lie algebras, and for such classes the property of nilpotency (when it exists) is preserved.*

Proof. For continuity we will use the same notation as in theorem 6·3. Letting $\hat{\epsilon}_R \in \mathrm{Hom}_{\mathbf{Z}}(\overline{U} \otimes_{\mathbf{Z}} \overline{U}, \Omega_1(U))$, $\hat{\gamma}_A \in \mathrm{Hom}_{\mathbf{F}_p[T]}(\overline{V} \otimes_{\mathbf{F}_p[T]} \overline{V}, \Omega_1(V))$ with $\hat{\epsilon}_R\theta = \hat{\gamma}_A$, we first show that $\hat{\epsilon}_R$ factors through $\bigwedge_2(\overline{U})$ if and only if $\hat{\gamma}_A$ factors through $\bigwedge_2(\overline{V})$. If we let $1 \leq j, k \leq t$ then it follows from the definition of θ that

$$(\overline{u}_j \otimes \overline{u}_k)\hat{\epsilon}_R = -(\overline{u}_k \otimes \overline{u}_j)\hat{\epsilon}_R \quad \text{if and only if} \quad (\overline{v}_j \otimes \overline{v}_k)\hat{\gamma}_A = -(\overline{v}_k \otimes \overline{v}_j)\hat{\gamma}_A$$

and

$$(\overline{u}_j \otimes \overline{u}_j)\widehat{\epsilon}_R = 0 \quad \text{if and only if} \quad (\overline{v}_j \otimes \overline{v}_j)\widehat{\gamma}_A = 0\,.$$

The result follows immediately from this.

We now show that the Jacobi identity holds in the Lie ring R if and only if the Jacobi identity holds in the $\mathbf{F}_p[T]$−algebra A. For elements $x, y, z \in R$ and $a, b, c \in A$ let

$$J_R(x,y,z) = [x,y,z]_R + [y,z,x]_R + [z,x,y]_R$$

and

$$J_A(a,b,c) = [a,b,c]_A + [b,c,a]_A + [c,a,b]_A\,,$$

and observe that the Jacobi identity holds in R if and only if $J_R(u_j, u_k, u_l) = 0$ for each $j,k,l = 1,\ldots,t$, and the Jacobi identity holds in A if and only if $J_A(v_j, v_k, v_l) = 0$ for each $j,k,l = 1,\ldots,t$. Now if $\lambda_t \geq 2$ then $\Omega_1(U) \subseteq \mathfrak{U}_1(U)$ and $\Omega_1(V) \subseteq \mathfrak{U}_1(V)$ which implies that for any $j,k,l = 1,\ldots,t$ we would have $[u_j, u_k]_R \in \mathfrak{U}_1(U)$ and $[v_j, v_k]_A \in \mathfrak{U}_1(V)$ so that $[u_j, u_k, u_l]_R = 0$ and $[v_j, v_k, v_l]_A = 0$, thereby implying that the Jacobi identity holds in both R and A. So we may assume that $\lambda_t = 1$ and recall from the proof of theorem 6·3 that d_r is defined to be the number of type invariants equal to $\lambda_{t_r} = \lambda_t$. Observe that if we let $1 \leq j,k \leq t$ then since $\widehat{\epsilon}_R\theta = \widehat{\gamma}_A$ it follows that there exist integers $\{\alpha_{jk}^e\}_{e=1}^t$ such that

$$[u_j,u_k]_R = \sum_{e=1}^{t} \alpha_{jk}^e p^{\lambda_e - 1} u_e \qquad \text{and} \qquad [v_j,v_k]_A = \sum_{e=1}^{t} \alpha_{jk}^e T^{\lambda_e - 1} v_e \tag{6·4}$$

Now letting $1 \leq j,k,l \leq t$ be arbitrary, we see that since $\lambda_e - 1 \geq 1$ for $1 \leq e \leq t - d_r$ and $\lambda_e - 1 = 0$ for $t - d_r + 1 \leq e \leq t$, it follows that

$$\begin{aligned} [u_j,u_k,u_l]_R &= \sum_{e=t-d_r+1}^{t} \alpha_{jk}^e [u_e,u_l]_R = \sum_{e=t-d_r+1}^{t} \alpha_{jk}^e \Big(\sum_{f=1}^{t} \alpha_{el}^f p^{\lambda_f - 1} \Big) u_f \\ &= \sum_{f=1}^{t} \Big(\sum_{e=t-d_r+1}^{t} \alpha_{jk}^e \alpha_{el}^f \Big) p^{\lambda_f - 1} u_f \end{aligned} \tag{6·5}$$

and

$$[v_j,v_k,v_l]_A = \sum_{f=1}^{t} \Big(\sum_{e=t-d_r+1}^{t} \alpha_{jk}^e \alpha_{el}^f \Big) T^{\lambda_f - 1} v_f \tag{6·6}$$

By permuting j,k,l cyclically in (6·5) and (6·6) we obtain

$$J_R(u_j,u_k,u_l) \quad = \quad \sum_{f=1}^{t}\Big(\sum_{e=t-d_r+1}^{t}\alpha_{jk}^{e}\alpha_{el}^{f}+\alpha_{lj}^{e}\alpha_{ek}^{f}+\alpha_{kl}^{e}\alpha_{ej}^{f}\Big)p^{\lambda_f-1}u_f$$

and

$$J_A(v_j,v_k,v_l) \quad = \quad \sum_{f=1}^{t}\Big(\sum_{e=t-d_r+1}^{t}\alpha_{jk}^{e}\alpha_{el}^{f}+\alpha_{lj}^{e}\alpha_{ek}^{f}+\alpha_{kl}^{e}\alpha_{ej}^{f}\Big)T^{\lambda_f-1}v_f\,,$$

from which it follows that $J_R(u_j,u_k,u_l)=0$ if and only if $J_A(v_j,v_k,v_l)=0$, as required. Therefore we have shown that $\widehat{\epsilon}_R$ defines a Lie ring structure on U if and only if $\widehat{\gamma}_A$ defines an $\mathsf{F}_p[T]-$Lie algebra structure on V. Therefore θ induces a one-to-one correspondence between isomorphism classes of Lie rings in $\mathcal{R}_n^p(\lambda_1,\ldots,\lambda_t)$ and isomorphism classes of $\mathsf{F}_p[T]-$Lie algebras in $\mathcal{A}_n^p(\lambda_1,\ldots,\lambda_t)$.

To complete the proof we must show that nilpotency (when it exists) is also preserved in this correspondence. Suppose first that $\widehat{\epsilon}_R$ and $\widehat{\gamma}_A$ are arbitrary and correspond under θ. Then $R/\mathfrak{U}_1(R)$ is an F_p-algebra and $A/\mathfrak{U}_1(A)$ is an $\mathsf{F}_p[T]-$algebra annihilated by T, i.e. an F_p-algebra, and using the fact that $\widehat{\epsilon}_R\theta=\widehat{\gamma}_A$ it follows that $R/\mathfrak{U}_1(R)\cong A/\mathfrak{U}_1(A)$ as F_p-algebras where the isomorphism takes the basis $(\overline{u}_1,\ldots,\overline{u}_t)$ onto $(\overline{v}_1,\ldots,\overline{v}_t)$ (to see this, consider the structure constants given by (6·4)). Now if, in addition, R is a Lie ring and A is an $\mathsf{F}_p[T]-$Lie algebra, then R is a nilpotent Lie ring if and only if $R/\mathfrak{U}_1(R)$ is a nilpotent F_p-Lie algebra, and A is a nilpotent $\mathsf{F}_p[T]-$Lie algebra if and only if $A/\mathfrak{U}_1(A)$ is a nilpotent $\mathsf{F}_p[T]-$Lie algebra if and only if $A/\mathfrak{U}_1(A)$ is a nilpotent F_p-Lie algebra. The result follows from this. □

We now have the following immediate corollary which is the key result for the next section.

Corollary 6·6. *Let p be a prime and n a natural number.*

i) For any partition $\lambda_1\geq\cdots\geq\lambda_t$ of n, there is a one-to-one correspondence between isomorphism classes of nilpotent Lie rings in $\mathcal{R}_n^p(\lambda_1,\ldots,\lambda_t)$ and isomorphism classes of nilpotent $\mathsf{F}_p[T]/(T^n)-$Lie algebras in $\mathcal{A}_n^p(\lambda_1,\ldots,\lambda_t)$.

ii) There is a one-to-one correspondence between isomorphism classes of nilpotent Lie rings in $\mathcal{R}_n^p$ and isomorphism classes of nilpotent $\mathsf{F}_p[T]/(T^n)-$Lie algebras in $\mathcal{A}_n^p$. □

We conclude this section by showing that in the correspondence we established between $\mathcal{R}_n^p$ and $\mathcal{A}_n^p$ there is no way of associating morphisms to give a functorial isomorphism when $p \geq n \geq 3$. To see this, let

$$U = \mathbb{Z}/p^n\mathbb{Z} \qquad \text{and} \qquad V = \mathbb{F}_p[T]/(T^n),$$

and observe that there is one Lie ring structure on U and one $\mathbb{F}_p[T]-$Lie algebra structure on V (they are both cyclic modules over $\mathbb{Z}$ and $\mathbb{F}_p[T]$ respectively, and so the structure must be Abelian). If the correspondence was an isomorphism then the automorphism group of the Lie ring on U would be isomorphic to the automorphism group of the $\mathbb{F}_p[T]-$Lie algebra on V, and since the structures are both Abelian these groups just coincide with the automorphism group of the underlying module which, in the case of U is the group of units of $\mathbb{Z}/p^n\mathbb{Z}$, and in the case of V is the group of units of $\mathbb{F}_p[T]/(T^n)$. Now since we are assuming that $p \geq 3$ it follows that $\mathbb{Z}/p^n\mathbb{Z}^\times$ is cyclic of order $p^{n-1}(p-1)$, but if $f \in \mathbb{F}_p[T]$ with constant term $\not\equiv 0$ modulo p, then $f^{p(p-1)} \equiv 1 \pmod{T^n}$ and so the group of units of $\mathbb{F}_p[T]/(T^n)$ has exponent dividing $p(p-1)$ but has order $p^{n-1}(p-1)$, therefore cannot be cyclic.

Remark. It is interesting to note that when $n = 2$, $\mathbb{Z}/p^n\mathbb{Z}$ and $\mathbb{F}_p[T]/(T^n)$ are isomorphic as ***multiplicative monoids***, for any prime p. To see this, observe that $\mathbb{Z}/p^2\mathbb{Z}^\times$ is cyclic of order $p(p-1)$, and so we can choose an integer α such that $\alpha + p^2\mathbb{Z}$ is a generator of $\mathbb{Z}/p^2\mathbb{Z}^\times$, which implies that α^p has order $p-1$ modulo p^2 and generates $\mathbb{Z}/p\mathbb{Z}^\times$. It then follows that the element $\alpha^p(1+p)+p^2\mathbb{Z}$ has order $p(p-1)$ and, identifying $\mathbb{F}_p$ with $\mathbb{Z}/p\mathbb{Z}$, we have a map

$$\begin{aligned} \pi \;:\; & \mathbb{Z}/p^2\mathbb{Z}^\times & \longrightarrow \quad & \mathbb{F}_p[T]/(T^2)^\times \\ : \; & \alpha^{pk}(1+p)^k + p^2\mathbb{Z} & \longmapsto \quad & \alpha^{pk}(1+kT) + (T^2), \qquad 0 \leq k < p(p-1) \end{aligned}$$

and since $\alpha^p(1+T)+(T^2)$ has order $p(p-1)$ this is a group isomorphism. We extend this map to the non-units by defining

$$\begin{aligned} \pi \;:\; & 0 + p^2\mathbb{Z} & \longmapsto \quad & 0 + (T^2) \\ : \; & \alpha^{pk}p + p^2\mathbb{Z} & \longmapsto \quad & \alpha^{pk}T + (T^2), \qquad 0 \leq k < p-1 \end{aligned}$$

which gives a monoid isomorphism.

Section 6·3. Proofs of the Main Results.

We now apply the results of the previous section to prove theorems 6·1 and 6·2 which were stated in the introduction. Recall that if p is a prime greater than or equal to the natural number n, then any group of order p^n belongs to the category Γ_p and has a sequence of type invariants associated to it.

Proposition 6·7. *Let p be a prime greater than or equal to the natural number n and suppose that $\lambda_1 \geq \cdots \geq \lambda_t$ is a partition of n. Then there is a one-to-one correspondence between isomorphism classes of groups of order p^n which are of type $(\lambda_1, \ldots, \lambda_t)$ and whose derived subgroup has exponent dividing p, and isomorphism classes of nilpotent $\mathsf{F}_p[T]/(T^n)-$Lie algebras L of type $(\lambda_1, \ldots, \lambda_t)$ in which $T[L, L] = 0$.*

Proof. Recall from section 1·1·3 that we have mutually inverse functors $\mathcal{L}_p$ and $\mathcal{G}_p$ between the categories Γ_p and Λ_p given by the Campbell-Hausdorff formula and Lazard's inversion formulas. Moreover, if P is in Γ_p then the derived subgroup of P coincides with the derived subring of $\mathcal{L}_p(P)$ and since the functors preserve the order of an element, it follows that the exponent of the derived subgroup of P coincides with the additive exponent of $\big[\mathcal{L}_p(P), \mathcal{L}_p(P)\big]$. Therefore since the type invariants of P coincide with the type invariants of $\mathcal{L}_p(P)$, it follows that the category of groups of order p^n which are of *type* $(\lambda_1, \ldots, \lambda_t)$ and whose derived subgroup has exponent dividing p, is functorially isomorphic to the category of nilpotent Lie rings in $\mathcal{R}_n^p(\lambda_1, \ldots, \lambda_t)$. In particular, there is a one-to-one correspondence between the isomorphism classes in these two categories. The result then follows from part i) of corollary 6·6. □

Proof of theorem 6·1

Since, for $p \geq n$, the isomorphism classes of groups of order p^n, nilpotent Lie rings of order p^n and nilpotent $\mathsf{F}_p[T]/(T^n)-$Lie algebras of F_p-dimension n are partitioned by type invariants, the theorem follows from proposition 6·7. □

Remark. Observe that this correspondence is explicit in the sense that if we know the structure constants for the Lie ring $\mathcal{L}_p(P)$ relative to some basis of $\mathcal{L}_p(P)$, then we can construct a representative of the isomorphism class of $\mathsf{F}_p[T]/(T^n)-$Lie algebras corresponding

to P by using theorem 6·3. Now when the type invariants are all equal to 1 (i.e. when P has exponent p), the Lie ring $\mathcal{L}_p(P)$ has characteristic p and so is an F_p-Lie algebra. Moreover, the $\mathsf{F}_p[T]-$Lie algebra associated to it by theorem 6·3 is then annihilated by T and is therefore just an F_p-Lie algebra which is easily seen to be isomorphic to $\mathcal{L}_p(P)$. This comment was stated in the introduction.

Now if L is any nilpotent F_p-Lie algebra of F_p-dimension n then the isomorphism classes of nilpotent $\mathsf{F}_p[T]/(T^n)-$Lie algebra structures on L correspond to the orbits of the conjugation action of $\mathrm{Aut}_{\mathrm{Lie}}(L)$ on the set of nilpotent L-linear maps

$$\{\,\sigma \in \mathrm{Hom}_{\mathsf{F}_p}(L,L) \,:\, \sigma^n = 0 \text{ and } [x\sigma, y] = [x,y]\sigma \text{ for all } x,y \in L\,\}$$

(these maps give the possible $T-$actions), and an $\mathsf{F}_p[T]-$Lie algebra A arising from one of these linear maps σ satisfies the condition $T[A,A] = 0$ if and only if $\mathrm{Im}\,\sigma \subseteq Z(L)$. Observe also that the type invariants of the resulting $\mathsf{F}_p[T]/(T^n)-$module are precisely the dimensions of the Jordan blocks of σ, and so if, for a partition $\underline{\lambda} = (\lambda_1, \ldots, \lambda_t)$ of n, we denote by $C(L, \underline{\lambda})$ the nilpotent $L-$linear maps σ with $\mathrm{Im}\,\sigma \subseteq Z(L)$ and Jordan block dimensions $\underline{\lambda}$, then the number of isomorphism classes of nilpotent $\mathsf{F}_p[T]/(T^n)-$ Lie algebras on L of *type* $(\lambda_1, \ldots, \lambda_t)$ with $T[L,L] = 0$ is given by

$$\sum_{\sigma \in C(L,\underline{\lambda})} \frac{1}{\left|\sigma^{\mathrm{Aut}(L)}\right|}.$$

Now observe that an $\mathsf{F}_p[T]/(T^n)-$Lie algebra determines the isomorphism class of its underlying F_p-Lie algebra, and so it follows that if we denote by $\mathcal{K}_n^p$ a transversal for the isomorphism classes of nilpotent n-dimensional F_p-Lie algebras, then together with proposition 6·7 we have shown the following result

Proposition 6·8. *For $p \geq n$ and a partition $\underline{\lambda} = (\lambda_1, \ldots, \lambda_t)$ of n, the number of isomorphism classes of groups of order p^n which are of type $(\lambda_1, \ldots, \lambda_t)$ and whose derived subgroup has exponent dividing p is given by*

$$\sum_{L \in \mathcal{K}_n^p} \sum_{\sigma \in C(L, \underline{\lambda})} \frac{1}{\left| \sigma^{\mathrm{Aut}(L)} \right|}.$$

□

With this result and recalling the discussion of the functors $\mathcal{L}_p$ and $\mathcal{G}_p$ given in section 1·1·3 we can now prove theorem 6·2.

Proof of theorem 6·2

Fixing $p \geq n$ and letting $\mathcal{E}_n^p$ be a tranversal for the groups of order p^n and exponent p we know that the set of Lie algebras $\{ \mathcal{L}_p(E) : E \in \mathcal{E}_n^p \}$ given by the inversion formulas of Lazard, is a transversal for the isomorphism classes of nilpotent n-dimensional F_p−Lie algebras. Now if $E \in \mathcal{E}_n^p$ and σ is a nilpotent F_p−linear map $\mathcal{L}_p(E) \to \mathcal{L}_p(E)$ which commutes with the adjoint maps on $\mathcal{L}_p(E)$ and satisfies $\mathrm{Im}\,\sigma \subseteq Z(\mathcal{L}_p)$, then by the Campbell-Hausdorff formula (1·2) we see that σ is a group homomorphism $E \to E$ with $\mathrm{Im}\,\sigma \subseteq Z(E)$ and $\sigma^n = e_E$, so that $\sigma \in N_E$. Conversely, given any element $\sigma \in N_E$ we see that σ is a nilpotent Lie ring endomorphism of $\mathcal{L}_p(E)$ with $\mathrm{Im}\,\sigma \subseteq Z(\mathcal{L}_p(E))$, and if $x, y \in \mathcal{L}_p(E)$ then $[x,y]\sigma = [x\sigma, y\sigma] = 0 = [x\sigma, y]$, so that σ is $\mathcal{L}_p(E)$−linear. It therefore follows that for $E \in \mathcal{E}_n^p$ we have

$$N_E = \bigcup_{\substack{\text{partitions} \\ \underline{\lambda} \text{ of } n}} C(\mathcal{L}_p(E), \underline{\lambda})$$

The required formula follows from this by summing the formula given in proposition 6·8 over all partitions of n and using the fact that the automorphism group of an element E of $\mathcal{E}_n^p$ coincides with the automorphism group of the Lie ring $\mathcal{L}_p(E)$. □

Section 6·4. Some Remarks on Groups of Order p^7.

In the literature, classifications of groups of order p^n for all primes p and $n \leq 6$ are to be found in [6] (in the case of $p = 2$), and in [12] (in the case of $p \geq 3$). The situation for $n = 7$ is not so complete with classifications published for $p = 2$ in [13], and in [30] for the groups of order p^7 and exponent p (p an arbitrary prime). In view of this, we collate here the information concerning groups of order p^7 contained in this thesis (together with some other known cases). Since we will only be discussing regular p-groups we will use the notation already introduced in chapter 4, i.e. given a partition $k \geq \lambda_1 \geq \ldots \geq \lambda_t$ of 7 and a prime p, we denote by $\Psi_k^p(\lambda_1, \ldots, \lambda_t)$ the number of regular p-groups of order p^7 and *type* $(k, \lambda_1, \ldots, \lambda_t)$. We arrange this summary by decreasing exponent.

Exponent p^7

For any prime p there is only one group here.

Exponents p^6 and p^5

For any prime p, the groups of order p^7 and exponent p^6 or p^5 can be obtained from Burnside's book [3] and Miller's paper [21] as a consequence of their work on p-groups of coexponent ≤ 2. For $p \geq 5$ these groups are regular (this follows from theorem 2·1) and correspond to the partitions $(6,1), (5,2)$ and $(5,1,1)$ of 7. In calculations not included in this thesis we have verified their formulas for $p \geq 5$ and include them here for completeness

$$\begin{aligned} \Psi_6^p(1) &= 2 \\ \Psi_5^p(2) &= 5 \\ \Psi_5^p(1,1) &= 7 \end{aligned}$$

Exponent p^4

In chapter 5 we showed that the following formulas hold for the number of groups of order p^7 and exponent p^4 (for $p \geq 5$)

$$\begin{aligned} \Psi_4^p(1,1,1) &= 23 + 2(p-1,3) + (p-1,4) \\ \Psi_4^p(2,1) &= 5p + 30 \\ \Psi_4^p(3) &= 6 \end{aligned}$$

Moreover, for the partitions $(4,2,1)$ and $(4,3)$ we gave an explicit determination of the corresponding Lie rings which, in theory, gives a classification of the groups by using the functors $\mathcal{L}_p$ and $\mathcal{G}_p$ to derive any structural information.

Exponents p^3 and p^2

We now turn to the groups of order p^7 which have exponent less than p^4 and assume that $p \geq 7$ so that regularity is automatic, and consider first the groups of *type* $(3,1,1,1,1)$. Now the coexponent of such a group is 4 and so since we are assuming that $p > 2(f-1)$ we can apply theorem 4·10 to deduce that

$$\Psi_3^p(1,1,1,1) = \Psi_2^p(1,1,1,1),$$

thus reducing the problem to a determination of certain groups of order p^6. Now the groups of order p^6 have appeared in [12] and he tabulates them by type invariants so in principal one could produce a formula for $\Psi_3^p(1,1,1,1)$ from this paper, although the list of groups of order p^6 given in [12] is known to contain mistakes (this is remarked in [24]).

Now consider (for $p \geq 7$) the groups of order p^7 which are of *type* $(2,1,1,1,1,1)$ or *type* $(2,2,1,1,1)$. In such a group P, $P/\Omega_1(P)$ has order p or p^2 and so is Abelian. Therefore $P_2 \subseteq \Omega_1(P)$ and so the exponent of P_2 divides p. Hence proposition 6·8 gives us

the following "formulas" for $\Psi_2^p(1,1,1,1,1)$ and $\Psi_2^p(2,1,1,1)$

$$\begin{aligned}\Psi_2^p(1,1,1,1,1) &= \sum_{L\in\mathcal{K}_7^p} \sum_{\sigma\in C\left(L,(2,1,1,1,1,1)\right)} \frac{1}{\left|\sigma^{\mathrm{Aut}(L)}\right|} \\ \Psi_2^p(2,1,1,1) &= \sum_{L\in\mathcal{K}_7^p} \sum_{\sigma\in C\left(L,(2,2,1,1,1)\right)} \frac{1}{\left|\sigma^{\mathrm{Aut}(L)}\right|}\end{aligned} \tag{6·7}$$

These formulas are summing over the 7-dimensional nilpotent F_p-Lie algebras which are known by Wilkinson's work [30], and he has shown that the number of such algebras depends on p, therefore the number of terms in these formulas depends on p.

For the remaining partitions $(2,2,2,1)$, $(3,3,1)$, $(3,2,2)$ and $(3,2,1,1)$, the exponent of the derived subgroup of the corresponding groups is at most p^2, and there clearly exist groups of each type with commutators of order p^2. Therefore for these partitions, the analogous formulas to (6·7) only give us partial information. In the light of theorem 6·1 a natural question to ask (with these groups in mind) is whether theorem 6·1 holds under the weaker hypotheses that the groups have derived subgroup whose exponent divides p^2, and the nilpotent $\mathsf{F}_p[T]/(T^n)-$Lie algebras L satisfy $T^2[L,L]=0$. However, it seems unlikely that trying to prove this in a similar manner to theorem 6·1 by merely viewing the structure constants arising from a ring R of order p^n with $p^2[R,R]=0$ as polynomials in p with coefficients reduced modulo p, and then reinterpreting these as polynomials in T by setting p equal to T in order to obtain an $\mathsf{F}_p[T]/(T^n)-$algebra A with $T^2[A,A]=0$, is going to succeed since the change of basis action will involve comparing solutions to congruences modulo p^2 with solutions of congruences modulo T^2 and these rings have different characteristics (although multiplicatively isomorphic).

Exponent p

These are known for any prime p from Wilkinson's work [30].

References

[1] H. Bender, A determination of the groups of order p^5, Ann. of Math. (2) **29**, 61–94 (1927).

[2] N. Blackburn, On a special class of p-groups, Acta. Math. **100**, 45–92 (1958).

[3] W. Burnside, Theory of Groups of Finite Order, Cambridge University Press, 1911.

[4] P. M. Cohn, Algebra Volume 2 second edition, John Wiley and Sons, 1989.

[5] M. Hall, Jr., A basis for free Lie rings and higher commutators in free groups, Proc. Amer. Math. Soc. **1**, 575–581 (1950).

[6] M. Hall, Jr., and J. K. Senior, The groups of order 2^n ($n \leq 6$), Macmillan, New York, 1964.

[7] P. Hall, A contribution to the theory of groups of prime-power order, Proc. London Math. Soc (2) **36**, 29–95 (1933).

[8] P. Hall, On a theorem of Frobenius, Proc. London Math. Soc. (2) **40**, 468–507 (1936).

[9] B. Huppert, Endliche Gruppen I, Die Grundlehren der Mathematischen Wissenschaften 134, Springer-Verlag, Berlin and New York, 1967.

[10] B. Huppert and N. Blackburn, Finite Groups II, Die Grundlehren der Mathematischen Wissenschaften 242, Berlin, Heidelberg, New York, 1982.

[11] N. Jacobson, Lie Algebras, Wiley-Interscience, 1962.

[12] R. James, The Groups of Order p^6 (p an odd prime), Math. Comput. **34**, 613–637 (1980).

[13] R. James, M. F. Newman and E. A. O'Brien, The groups of order 128, J. Alg. **129**, 136–158 (1990).

[14] D. L. Johnson, Presentations of Groups. London Mathematical Society Student Texts **15**, Cambridge University Press, 1990.

[15] M. Lazard, Sur les groupes nilpotents et les anneaux de Lie, Ann. Sci École Norm. Sup. **71**, 101–190 (1954).

[16] C. R. Leedham-Green and M. F. Newman, Space groups and groups of prime-power order. I, Arch. Math. **35**, 193–202 (1980).

[17] W. Magnus, Beziehungen zwischen Gruppen und Idealen in einem speziellen Ring, Math. Ann. **111**, 259–280 (1935).

[18] W. Magnus, Über Beziehungen zwischen höheren Kommutatoren, J. Reine Angew. Math. **177**, 105–115 (1937).

[19] W. Magnus, Über Gruppen und zugeordnete Liesche Ringe, J. Reine Angew. Math. **182**, 142–149 (1940).

[20] A. I. Mal'cev, Nilpotent torsion-free groups, Izv. Akad. Nauk. SSSR Ser. Mat. **13**, 201–202 (1949).

[21] G. A. Miller, On the groups of order p^m which contain operators of order p^{m-2}, Trans. Am. Math. Soc. **26**, 383–387 (1902).

[22] J. Moody, Private communication, (1991).

[23] L. I. Neikirk, Groups of order p^m, which contain cyclic subgroups of order p^{m-3}, Trans. Am. Math. Soc. **6** 316–325, (1905).

[24] M. F. Newman, Groups of prime-power order, in Groups — Canberra 1989; ed. by L. G. Kovács; Lecture Notes in Math. **1456**, pp. 49–62, Springer-Verlag, Berlin, Heidelberg, New York, London, Paris, Tokyo, Hong Kong, Barcelona, 1990.

[25] P. J. Sanders and T. S. Wilde, The Class and Coexponent of a Finite p-group, Warwick preprints 25/1994, University of Warwick, 1994.

[26] O. Schreier, Über die Erweiterung von Gruppen II, Hamburg Abh. **4**, 321–346 (1926).

[27] A. Shalev, The structure of finite p-groups: effective proof of the coclass conjectures, Invent. math. **115**, 315–345 (1994).

[28] M. Suzuki, Group Theory II, Grundlehren der Mathematischen Wissenschaften 248, Springer-Verlag, New-York, Berlin, Heidelberg and Tokyo, 1986.

[29] G. N. Titov, Groups containing a cyclic subgroup of index p^3, Mat. Zametki **28**, no. 1, 17–24, 167 (1980), (Russian). English Translation : Math. Notes **28** (1980), nos. 1–2, 472–476 (1981).

[**30**] D. F. Wilkinson, The groups of order p^7 (p any prime), J. Algebra **118**, 109–119 (1988).

[**31**] E. Witt, Treue Darstellung Liescher Ringe, J. Reine Angew Math. **177**, 152–160 (1937).

THE BRITISH LIBRARY
BRITISH THESIS SERVICE

TITLE PRIME-POWER LIE ALGEBRAS AND FINITE P-GROUPS.

AUTHOR Paul Jonathon SANDERS

DEGREE Ph.D

AWARDING BODY Warwick University

DATE 1994

THESIS NUMBER DX187307

THIS THESIS HAS BEEN MICROFILMED EXACTLY AS RECEIVED

The quality of this reproduction is dependent upon the quality of the original thesis submitted for microfilming. Every effort has been made to ensure the highest quality of reproduction. Some pages may have indistinct print, especially if the original papers were poorly produced or if awarding body sent an inferior copy. If pages are missing, please contact the awarding body which granted the degree.

Previously copyrighted materials (journals articles, published texts etc.) are not filmed.

This copy of the thesis has been supplied on condition that anyone who consults it is understood to recognise that it's copyright rests with its author and that no information derived from it may be published without the author's prior written consent.

Reproduction of this thesis, other than as permitted under the United Kingdom Copyright Designs and Patents Act 1988, or under specific agreement with the copyright holder, is prohibited.